PLAN DU SOUS SAVOIR S31

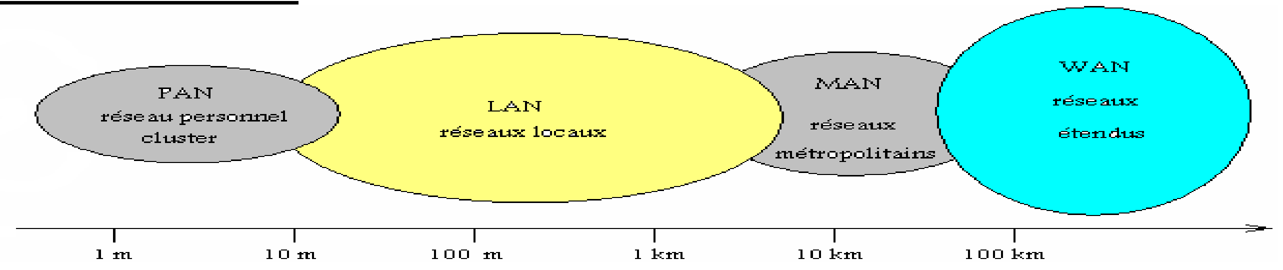
A . Terminologie des réseaux

1 . Définition des réseaux informatiques.

Un réseau informatique est un moyen qui permet à des individus ou à des groupes d'individus de partager des informations et des services. Les services que les réseaux offrent font partie de la vie courante des entreprises et administrations (banques, gestion, commerce, bases de données, recherche, etc...) et des particuliers (messagerie, loisirs, services d'informations et Internet ...).

On peut classer les réseaux en deux catégories avec fil et sans fil :

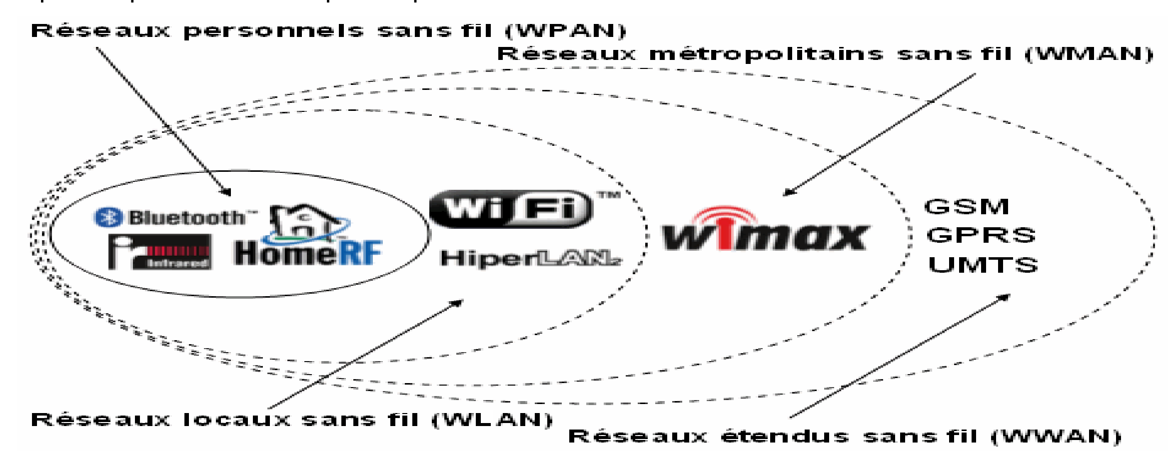
2 . Les réseaux avec fil.



- **Un *réseau personnel* (PAN : Personnal Area Network)** interconnecte des équipements personnels comme un ordinateur portable, un agenda électronique...
- **Un *réseau local* (LAN : Local Area Network**) peut s'étendre de quelques mètres à quelques kilomètres et correspond au réseau d'une entreprise. Il peut se développer sur plusieurs bâtiments et permet de satisfaire tous les besoins internes de cette entreprise.
- **Un *réseau métropolitain* (MAN : Metropolitan Area Network)** interconnecte plusieurs lieux situés dans une même ville, par exemple les différents sites d'une université ou d'une administration, chacun possédant son propre réseau local.
- **Un *réseau étendu* (WAN : Wide Area Network)** permet de communiquer à l'échelle d'un pays ou de la planète entière, les infrastructures physiques pouvant être terrestres ou spatiales à l'aide de satellites de télécommunications.
- **Un *réseau de stockage* (SAN : Storage Area Network)** est un réseau à haute performance dédié au transfert haut débit des données entre des serveurs et des ressources de stockage (disques durs).
- **Un *réseau privé virtuel* (VPN : Virtual Private Network)** est un réseau privé construit au sein du réseau publique mondial Internet. Au moyen d'un réseau privé virtuel, un télétravailleur peut accéder à distance au réseau sa société.

3. Les réseaux sans fil.

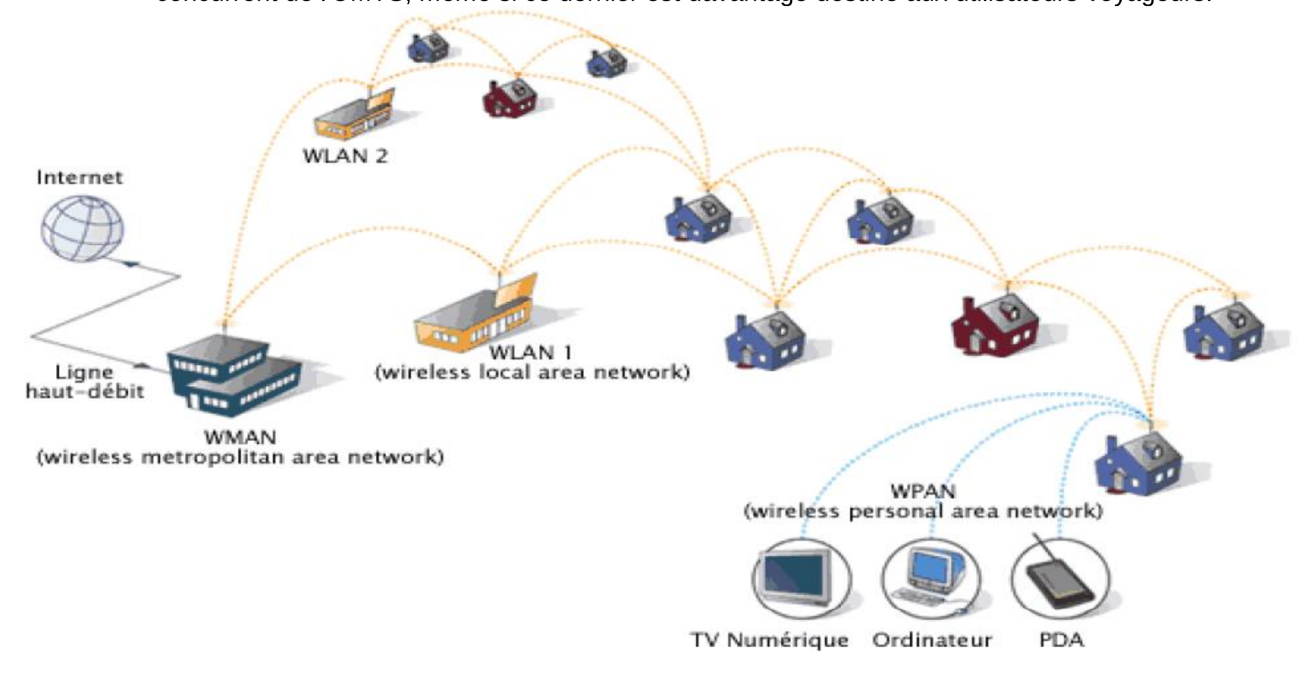
Un réseau sans fil (en anglais wireless network) est, comme son nom l'indique, un réseau dans lequel au moins deux terminaux peuvent communiquer sans liaison filaire. Grâce aux réseaux sans fil, un utilisateur a la possibilité de rester connecté tout en se déplaçant dans un périmètre géographique plus ou moins étendu, c'est la raison pour laquelle on entend parfois parler de "mobilité".



- **Un réseau personnel sans fil (WPAN : Wireless Personal Area Network)** concerne les réseaux sans fil d'une faible portée : de l'ordre de quelques dizaines mètres. Ce type de réseau sert généralement à relier des périphériques (imprimante, téléphone portable, appareils domestiques, ...) à un ordinateur sans liaison filaire ou bien à permettre la liaison sans fil entre deux machines très peu distantes. Il existe plusieurs technologies utilisées pour les WPAN :

- La principale technologie WPAN est la technologie Bluetooth proposant un débit théorique de base de 1 Mbps pour une portée maximale d'une trentaine de mètres.
- HomeRF (pour Home Radio Frequency), propose un débit théorique de 10 Mbps avec une portée d'environ 50 à 100 mètres sans amplificateur
- Enfin les liaisons infrarouges permettent de créer des liaisons sans fil de quelques mètres avec des débits pouvant monter à quelques mégabits par seconde.

- **Un réseau local sans fil (WLAN : Wireless Local Area Network)** est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Il permet de relier entre-eux les terminaux présents dans la zone de couverture. Il existe plusieurs technologies concurrentes :
  - Le Wifi soutenu par l'alliance WECA (Wireless Ethernet Compatibility Alliance) offre des débits allant de 54Mbps sur une distance de plusieurs centaines de mètres.
  - hiperLAN2 (HIgh Performance Radio LAN 2.0), norme européenne élaborée par l'ETSI (European Telecommunications Standards Institute). HiperLAN 2 permet d'obtenir un débit théorique de 54 Mbps sur une zone d'une centaine de mètres dans la gamme de fréquence comprise entre 5 150 et 5 300 MHz.
- **Un réseau métropolitain sans fils WMAN** (Wireless Metropolitan Area Network) est connu sous le nom de Boucle Locale Radio (BLR) qui offre un débit utile de 1 à 10 Mbit/s pour une portée de 4 à 10 kilomètres, ce qui destine principalement cette technologie aux opérateurs de télécommunication.
- **Un réseau étendu sans fil (WWAN : Wireless Wide Area Network)** est également connu sous le nom de réseau cellulaire mobile. Il s'agit des réseaux sans fil les plus répandus puisque tous les téléphones mobiles sont connectés à ces réseaux. Les principales technologies sont les suivantes :
  - GSM (Global System for Mobile Communication ou en français Groupe Spécial Mobile)
  - GPRS (General Packet Radio Service)
  - UMTS (Universal Mobile Telecommunication System).
  - Wimax (Worldwide Interoperability for Microwave Access standard). Basé sur une bande de fréquence de 2 à 11 GHz, offrant un débit de 70 Mbits/s sur 50km de portée, certains le placent en concurrent de l'UMTS, même si ce dernier est davantage destiné aux utilisateurs voyageurs.



B . Les modèles OSI et TCP/IP

I . LE MODELE de référence OSI

1 . Description du modèle OSI (Open Systems Interconnection)

Le processus d'envoi de données à travers les réseaux peut être décomposé en plusieurs tâches :

- Reconnaissance des données.
- Segmentation des données en paquets plus faciles à traiter.
- Ajout d'informations de séquence et de contrôle d'erreurs.
- Ajout d'informations dans chaque paquet de données afin de définir l'emplacement des données et d'identifier l'émetteur et le récepteur
- Dépôt des données sur le réseau et envoi.

Le système d'exploitation réseau effectue chacune de ces tâches en suivant un ensemble de procédures strictes, appelées protocoles ou règles de conduite

En 1978, l'ISO (International Standard Organisation) publia un ensemble de recommandations sur une architecture réseau permettant la connexion de périphériques hétérogènes : modèle OSI.
En 1984, l'ISO publia une mise à jour du modèle qui est devenue une norme internationale.

2 . Analyse des rôles des 7 couches du modèle OSI

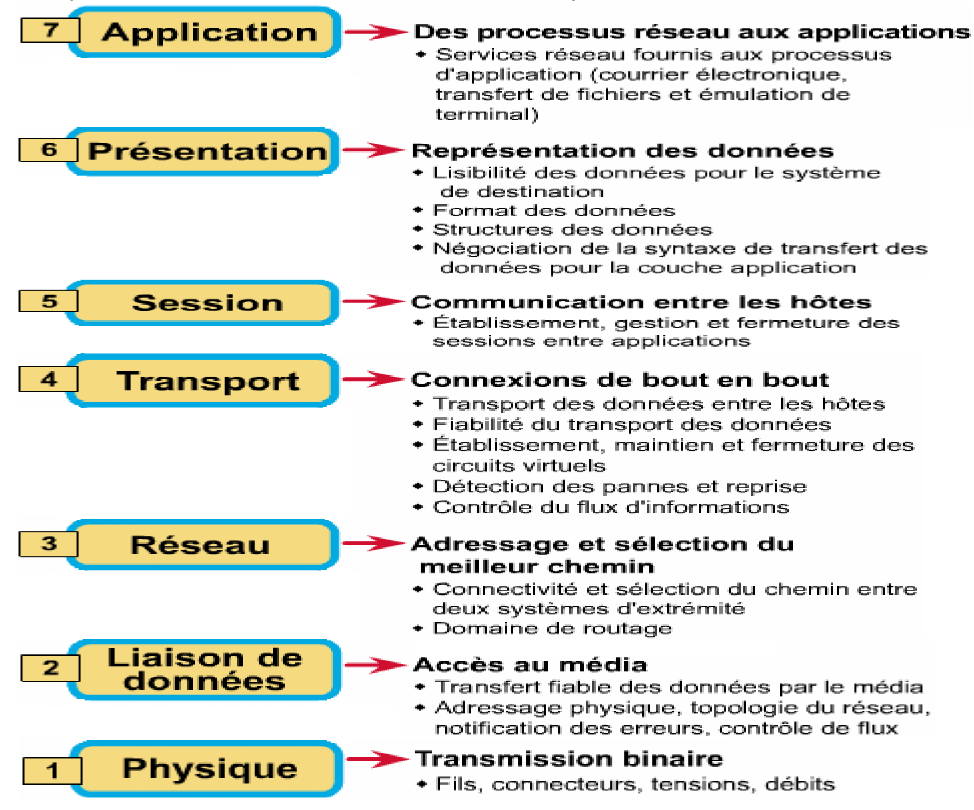
Le modèle de référence OSI comporte sept couches numérotées, chacune illustrant une fonction réseau bien précise. A chaque couche correspond des activités, des équipements ou des protocoles réseau différents.

7 Application
6 Présentation
5 Session
4 Transport
3 Réseau
2 Liaison de données
1 Physique

Le découpage du réseau en sept couches présente les avantages suivants :

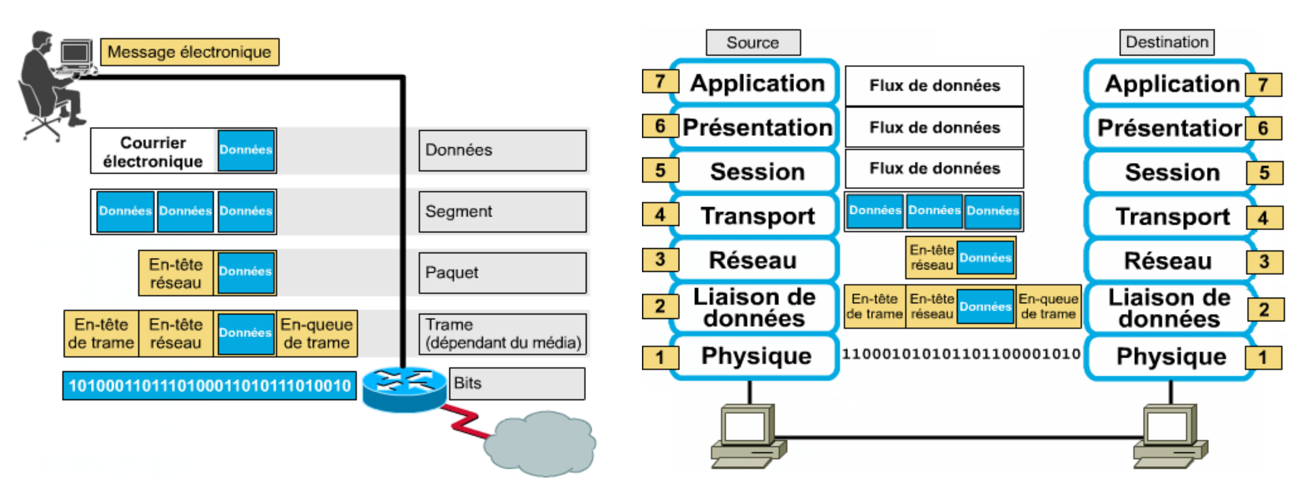
- Il divise les communications sur le réseau en éléments plus petits, ce qui permet de les comprendre plus facilement.
- Il empêche les changements apportés à une couche d'affecter les autres couches, ce qui assure un développement plus rapide.
- Il uniformise les éléments du réseau afin de permettre le développement et le soutien multiconstructeur.
- Il permet à différents types de matériel et de logiciel réseau de communiquer entre eux.

On utilise la phrase suivante comme aide-mémoire : Après Plusieurs Semaines Tout Respire La Pais



3 . Terminologie liée au modèle OSI

a. Exemple d'encapsulation des données



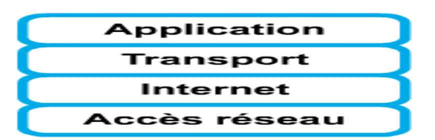
b. Répartition des éléments d'un réseau en fonction des couches du modèle OSI.

Couche n°	Nom	Unité d'encapsulation ou regroupement logique	Unités ou éléments fonctionnant au niveau de cette couche.
7	Application	Données	Logiciels
6	Présentation	Données	Logiciels
5	Session	Données	Logiciels
4	Transport	Segments	Routeur
3	Réseau	Paquets, datagrammes	Routeur
2	Liaison	Trames	Carte réseau, pont, commutateur
1	Physique	Bits	connecteurs, câbles, répéteur, concentrateur, MODEM

II . Description des quatre couches du modèle TCP/IP.

Le ministère américain de la Défense « *DOD* » a créé le modèle de référence TCP/IP parce qu'il avait besoin d'un réseau pouvant résister à toutes les conditions, même à une guerre nucléaire. Le ministère de la défense veut que ses paquets se rendent à chaque fois d'un point quelconque à tout autre point, peu importe les conditions. C'est ce problème de conception très épineux qui a mené à la création du modèle TCP/IP qui, depuis lors, est devenu la norme sur laquelle repose Internet.

Le modèle TCP/IP comporte quatre couches : la couche application, la couche transport, la couche *Internet* et la couche d'accès au réseau. Comme vous pouvez le constater, certaines couches du modèle TCP/IP portent le même nom que des couches du modèle OSI. Il ne faut pas confondre les couches des deux modèles, car la couche application comporte des fonctions différentes dans chaque modèle.



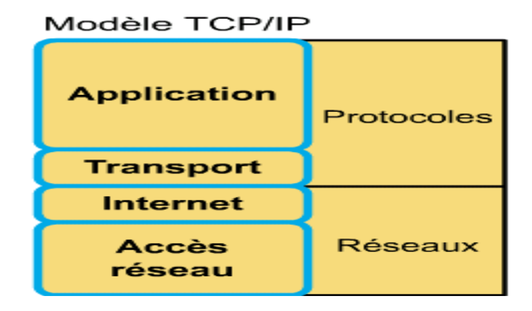
La couche application gère les protocoles de haut niveau : représentation codage et contrôle du dialogue. Le modèle TCP/IP regroupe en une seule couche tous les aspects liés aux applications.

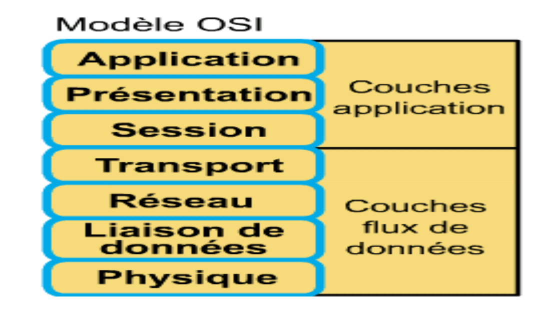
La couche transport est chargée de la fiabilité, du contrôle de flux et de la correction des erreurs. L'un de ses protocoles *TCP* est orienté connexion ce qui assure une transmission fiable des données en full duplex.

La couche Internet assure l'arrivée des paquets à leurs destinations indépendamment du trajet et des réseaux traversés pour y arriver. Le protocole qui régit cette couche est appelé protocole IP (Internet Protocol). L'identification du meilleur chemin et la commutation de paquets ont lieu au niveau de cette couche.

La couche d'accès au réseau se charge de tout ce dont un paquet IP a besoin pour établir une liaison physique. Cela comprend les détails sur les technologies LAN et WAN, ainsi que tous les détails dans les couches physique et liaison de données du modèle OSI.

III . Comparaison du modèle OSI et du modèle TCP/IP





En comparant le modèle OSI au modèle TCP/IP on remarque des similitudes et des différences :

Similitudes

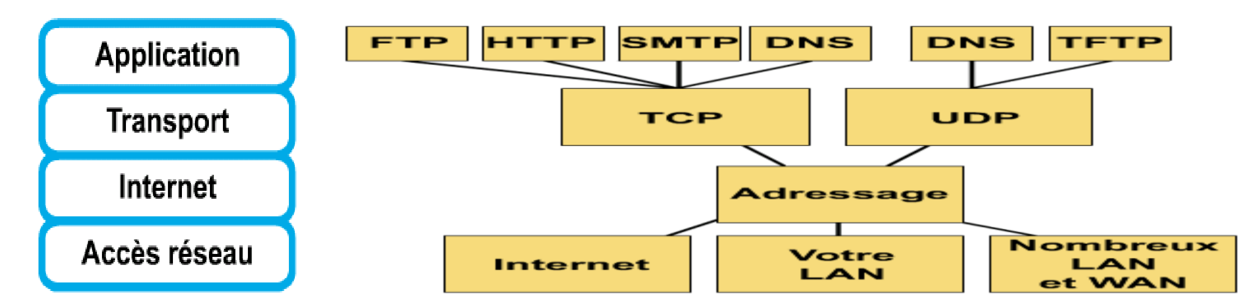
- Tous deux comportent des couches.
- Tous deux comportent une couche application, bien que chacune fournisse des services très différents.
- Tous deux comportent des couches réseau et transport comparables.
- Tous deux utilisent la technologie de commutation de paquets (et non de commutation de circuits).

Différences

- TCP/IP intègre la couche présentation et la couche session dans sa couche application.
- TCP/IP regroupe les couches physique et liaison de données OSI au sein d'une seule couche.
- TCP/IP semble plus simple, car il comporte moins de couches.
- Les protocoles TCP et IP constituent la norme sur laquelle s'est développé Internet. Aussi, le modèle TCP/IP a-t-il bâti sa réputation sur ses protocoles.

IV . Description des protocoles TCP/IP.

Le diagramme illustré dans la figure suivante est appelé *schéma de protocoles*. Il présente certains protocoles communs spécifiés par le modèle de référence TCP/IP.



Au niveau de la couche application, on trouve :

- FTP - Protocole de transfert de fichiers ou protocole FTP
- HTTP - Protocole HTTP (Hypertext Transfer Protocol)
- SMTP - Protocole SMTP (Simple Mail Transfer protocol)
- DNS - Système DNS (Domain Name System)
- TFTP - Protocole TFTP (Trivial File Transfer Protocol)

Le modèle TCP/IP met l'accent sur une souplesse maximale, au niveau de la couche application, à l'intention des développeurs de logiciels. La couche transport fait appel à deux protocoles : le protocole TCP (protocole de contrôle de transmission) et le *protocole UDP (User Datagram Protocol).*

Dans le modèle TCP/IP, IP (Internet Protocol) est le seul et unique protocole utilisé, et ce, quels que soient le protocole de transport utilisé et l'application qui demande des services réseau. Il s'agit là d'un choix de conception délibéré. *IP* est un protocole universel qui permet à tout ordinateur de communiquer en tout temps et en tout lieu.

C . Fonctionnalité et protocoles des couches applicatives

Voici une description des principaux protocoles utilisés dans cette couche :

1. HTTP (Hypertext Transfer Protocol):

Le protocole ***HTTP*** est le support du Web. Les pages Web sont créées avec un langage de formatage appelé HTML (*HyperText Markup Language*). Le code HTML indique au navigateur comment présenter une page Web pour obtenir un aspect particulier.
Les *liens hypertexte* (ou hyperliens) facilitent la navigation sur le Web. Il peut s'agir d'un objet, d'un mot, d'une phrase ou d'une image sur une page Web.

http://	www.	cisco.com	/edu/
Indique au navigateur le protocole à utiliser.	Indique le nom de l'hôte ou le nom d'un ordinateur précis.	Représente l'entité de domaine du site Web.	Spécifie le répertoire dans lequel la page Web est située sur le serveur. Ainsi, quand aucun nom n'est spécifié, le navigateur charge la page par défaut identifiée par le serveur.

Lorsque vous tapez une adresse, Le navigateur Web examine alors le protocole pour savoir s'il a besoin d'ouvrir un autre programme, puis détermine l'adresse IP du serveur Web à l'aide du système DNS. Ensuite, la couche transport établit une session avec le serveur Web.
Le serveur répond à la demande en transmettant au client Web tous les fichiers texte, audio, vidéo et graphique indiqués dans la page HTML. Le navigateur client rassemble tous ces fichiers pour créer une image de la page Web et met fin à la session.

2. DNS (Domain Name System):

Il est difficile de retenir l'adresse IP d'un site, car l'adresse numérique n'a aucun rapport apparent avec le contenu du site. ***DNS*** permet de convertir les @IP en des noms de domaine et l'inverse.
Il existe plus de 200 domaines de niveau supérieur sur Internet, notamment :

- **.us** – États-Unis
- **.fr** – France
- **.edu** – sites éducatifs
- **.com** – sites commerciaux …

3. FTP (File Transfer Protocol) et TFTP(Trivial File Transfer Protocol) :

FTP est un service orienté connexion fiable. L'objectif principal de ce protocole est d'échanger des fichiers dans les deux sens (importation et exportation) entre un ordinateur serveur et des ordinateurs clients en ouvrant une connexion.
TFTP est un service non orienté connexion. Il est utilisé sur les routeurs pour transférer des fichiers de configuration et des images système d'exploitation du routeur (IOS Cisco par exemple). Ce protocole, conçu pour être léger et facile à mettre en œuvre (il ne permet pas d'afficher le contenu des répertoires ni d'assurer l'authentification des utilisateurs).

4. SMTP (Simple Mail Transfer Protocol):

Les serveurs de messagerie communiquent entre eux à l'aide du protocole ***SMTP*** pour envoyer et recevoir des messages électroniques. Ce protocole transporte les messages à l'aide de TCP.
Les protocoles de client de messagerie les plus répandus sont POP3 et IMAP4, qui utilisent tous deux TCP pour transporter les données (récupérer les messages), par contre le client utilise toujours le protocole SMTP pour envoyer des messages.

5. SNMP (Simple Network Management Protocol) :

Le protocole ***SNMP*** est un protocole qui facilite l'échange d'information de gestion entre les équipements du réseau. Il permet aux administrateurs réseau de gérer les performances du réseau, de diagnostiquer et de résoudre les problèmes.

6. Telnet :

Le logiciel client ***Telnet*** permet de se connecter à un hôte Internet distant sur lequel est exécutée une application serveur Telnet, puis d'exécuter des commandes à partir de la ligne de commande.
Les opérations de traitement et de stockage sont entièrement exécutées par l'ordinateur distant.

D . Couche transport OSI

1. Introduction à la couche transport :

La couche transport a pour but :

- D'acheminer les données de la source à la destination. « TCP ou UDP »
- De contrôler le flux de ces données. « Fenêtrage »
- De garantir la fiabilité de ces données. « Accusés de réception »

Analogie : Imaginez une personne qui apprend une langue étrangère pour la première fois (il faut répéter les mots, parler lentement …)

La couche transport fait appel à deux protocoles : le protocole TCP (protocole de contrôle de transmission) et le *protocole UDP (User Datagram Protocol).*

2. Protocole TCP : (Transmission Control Protocol)

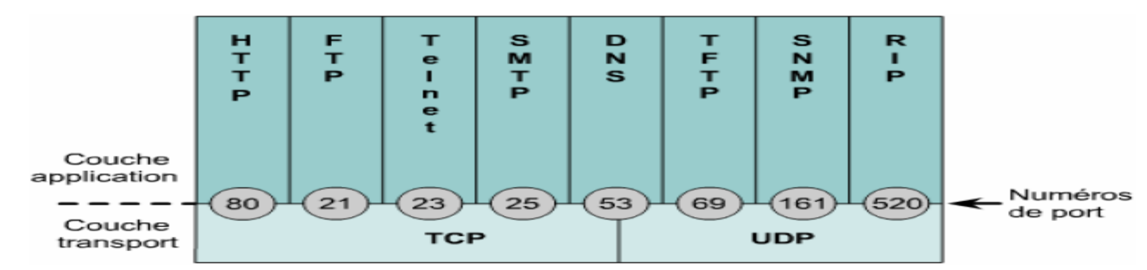
TCP (Transmission Control Protocol - protocole de contrôle de transmission), fournit d'excellents moyens pour créer, en souplesse, des communications réseau fiables, circulant bien et présentant un taux d'erreurs peu élevé. Le protocole TCP est orienté connexion. Il établit un dialogue sûr entre l'ordinateur source et l'ordinateur de destination, il a aussi pour fonction la division des données de la couche application en unités plus faciles à traiter appelées segments.
Les protocoles utilisant TCP sont les suivants: FTP, HTTP, SMTP, Telnet

3. Protocole UDP : (User Datagram Protocol)

C'est un protocole simple qui échange des datagrammes sans garantir leur bonne livraison.
UDP n'utilise ni fenêtres ni accusés de réception. La fiabilité est assurée par les protocoles de la couche application. Le protocole UDP est conçu pour les applications qui ne doivent pas assembler de séquences de segments.
Les protocoles utilisant UDP sont les suivants: TFTP, SNMP, DHCP, DNS.

4. Numéros de port TCP et UDP :

Les numéros de port servent à distinguer les différentes conversations qui circulent simultanément sur le réseau. Les développeurs d'applications ont convenu d'utiliser les numéros de port reconnus émis par l'IANA (Internet Assigned Numbers Authority).
Par exemple : **FTP** fait appel aux numéros de port standard 20 et 21. Le port 20 est utilisé pour la partie « données » et le port 21 pour le « contrôle ».

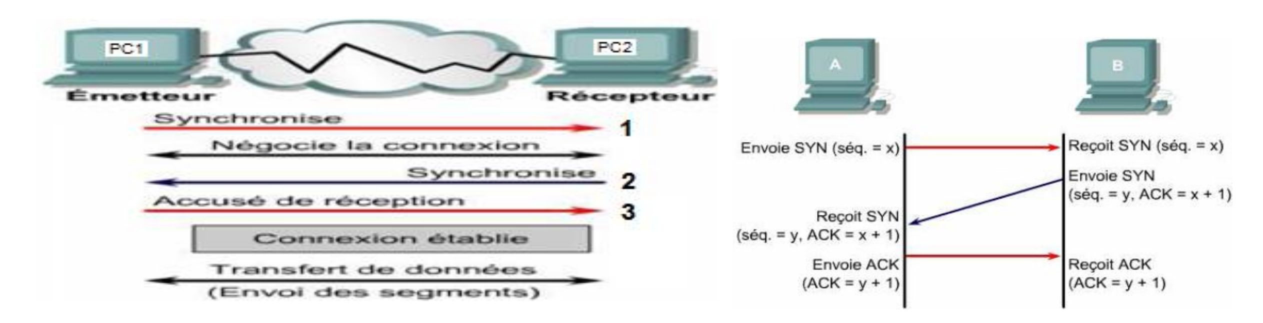


- Les numéros inférieurs à 1023 sont considérés comme des numéros de port reconnus.
- Les numéros supérieurs à 1024 sont des numéros attribués de manière dynamique.
- Les numéros de port enregistrés sont destinés à des applications spécifiques d'un fournisseur. La plupart se situent au-delà de 1024.
- Les systèmes d'extrémité utilisent les numéros de port pour sélectionner l'application appropriée. L'hôte source attribue dynamiquement des numéros de port source toujours supérieurs à 1023.

5. Établissement, maintien et fermeture de session

Lorsque l'ordinateur PC1 veut envoyer de l'information à l'ordinateur PC2, il doit tout d'abord établir une session avec ce dernier au niveau de la couche transport.

- Premièrement, PC1 envoie un message de synchronisation à PC2.
- PC2 reçoit le message, et négocie la connexion avec PC1, ensuite il va envoyer à son tour un message de synchronisation des paramètres négociés.
- PC1 envoie finalement un accusé de réception comme quoi la connexion est établit.
- A ce moment là, les deux ordinateurs peuvent échanger les données d'une façon bidirectionnelle.
- Une fois le transfert des données terminé, PC1 envoie un signal indiquant la fin de la transmission. PC2 accuse la réception et la connexion se termine.

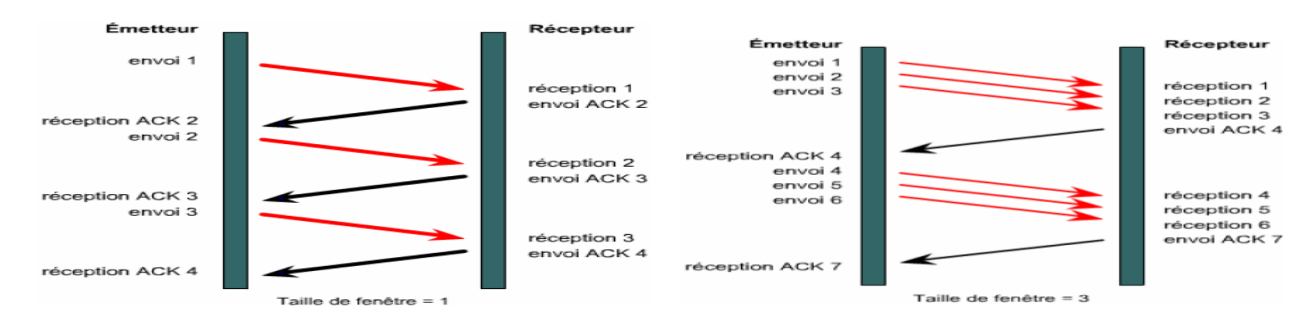


On parle alors d'échange en trois étapes (1 , 2 et 3)

Pour établir une connexion, les deux hôtes doivent synchroniser leurs numéros de séquence initiaux (**ISN** – Initial Sequence Number) : x pour A et y pour B

6. Le fenêtrage :

Le ***fenêtrage*** est une solution simple qui consiste, pour le destinataire, à accuser une réception à chaque transmission d'un nombre bien précis des segments.



Chaque protocole orienté connexion utilise une *taille de fenêtre* (la taille de la fenêtre indique le nombre des segments que l'hôte de destination est prêt à recevoir).

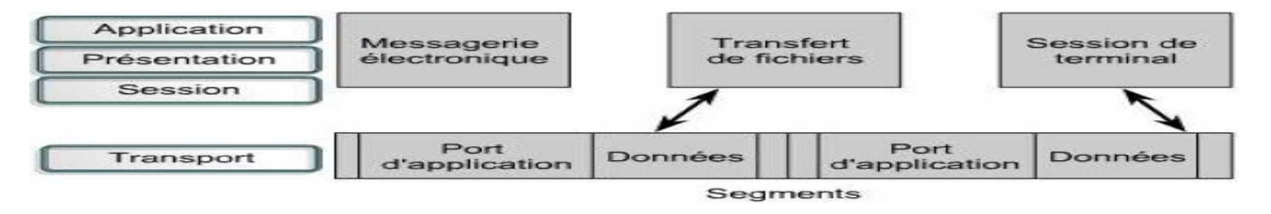
TCP utilise des accusés de réception prévisionnels. Cela signifie que le numéro de l'accusé indique le paquet suivant attendu.

Le fenêtrage fait référence au fait que la taille de la fenêtre est négociée de manière dynamique pendant la session TCP. Il constitue un mécanisme de contrôle de flux. C'est la machine de destination qui signale une taille de fenêtre à l'hôte source.

Chaque segment est numéroté avant la transmission pour pouvoir réassembler correctement les segments au niveau de la destination. (***Numéros des segments***)

7. Le multiplexage :

Plusieurs applications (pour chaque application un port différent) peuvent partager la même connexion de transport (ça veut dire qu'on peut utiliser deux services d'application ou plus en ouvrant une seule fois la connexion. On parle alors de *multiplexage des conversations de couche supérieure*.



8. Contrôle de flux :

Le contrôle de flux permet d'éviter le dépassement de capacité des mémoires tampons d'un hôte de destination. Pour ce faire, TCP met en relation les hôtes source et de destination qui conviennent alors d'un taux de transfert des données acceptable. Sinon, le destinataire va rejeter les segments.

La congestion peut se produire dans deux situations :

- Lorsqu'un ordinateur génère un trafic dont le débit est plus rapide que la vitesse du réseau.
- Lorsque plusieurs ordinateurs envoient simultanément des datagrammes à une même destination.

Pour éviter la perte des données, le processus TCP de PC2(récepteur) envoie un indicateur «***non prêt***» à PC1(émetteur), afin que ce dernier s'arrête de transmettre. Lorsque PC2 peut accepter de nouvelles données, il envoie l'indicateur de transport «***prêt***» à PC1 qui reprend alors la transmission des segments.

E . Couche réseau OSI

1. Introduction à la couche réseau :

Le rôle de la couche réseau, ou couche 3 OSI, consiste à sélectionner le meilleur chemin pour transférer les paquets sur le réseau. Elle fournit des services pour l'échange des éléments de données individuels sur le réseau entre des périphériques finaux identifiés. Pour effectuer ce transport de bout en bout, la couche 3 utilise quatre processus de base :

- l'adressage ;
- l'encapsulation ;
- le routage ;
- le décapsulage.

2. Protocoles de couche réseau du modèle OSI:

Les protocoles mis en œuvre dans la couche réseau qui transportent des données utilisateur comprennent :

- Protocole IP version 4 (IPv4)
- Protocole IP version 6 (IPv6)
- Protocole IPX de Novell
- AppleTalk
- CLNS (Connectionless Network Service)/DECNet

Le protocole IP (IPv4 et IPv6) constitue le protocole de transport de données de couche 3 le plus répandu et fait l'objet de ce cours. Les autres protocoles n'ont été que cités.

3. Protocoles de couche Internet du modèle TCP/IP :

Les protocoles de la couche Internet du protocole TCP/IP sont :

- IP assure l'acheminement au mieux (best-effort delivery) des paquets, non orienté connexion (n'effectue aucune vérification d'erreurs et ne fournit aucun service de correction). Il ne se préoccupe pas du contenu des paquets.
- ICMP (Internet Control Message Protocol) offre des fonctions de messagerie et de contrôle.
- ARP (Address Resolution Protocol) détermine les adresses de la couche liaison de données ou les @MAC pour les @IP connues.
- RARP (Reverse Address Resolution Protocol) détermine l'@ IP pour une @MAC connue.

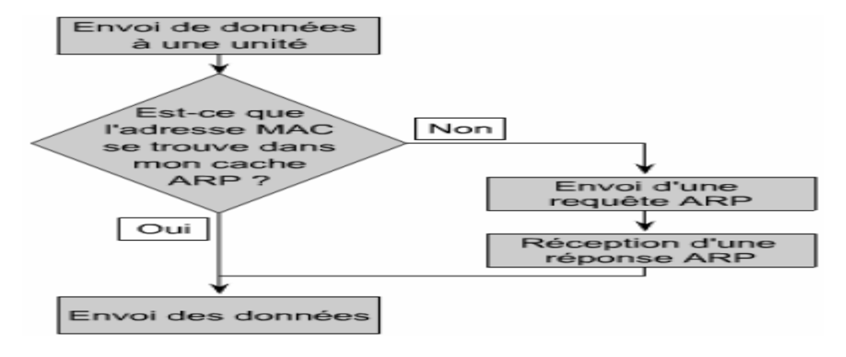
Le protocole IP effectue les opérations suivantes :

- Il définit un paquet et un système d'adressage.
- Il transfère des données entre la couche Internet et la couche d'accès au réseau.
- Il achemine des paquets à des hôtes distants.

Pour la structure de l'entête de ce protocole voir annexes.

4. Protocole ARP (Address Resolution Protocol)

Dans un réseau TCP/IP, un paquet de données doit contenir une adresse MAC de destination et une adresse IP de destination. Si l'une ou l'autre est manquante, les données qui se trouvent au niveau de la couche 3 ne sont pas transmises aux couches supérieures.
Les «***tables ARP***» sont stockées dans la mémoire RAM où les informations sont mises à jour automatiquement dans chaque équipement (correspondance @IP & @MAC pour les stations du même domaine de Broadcast).



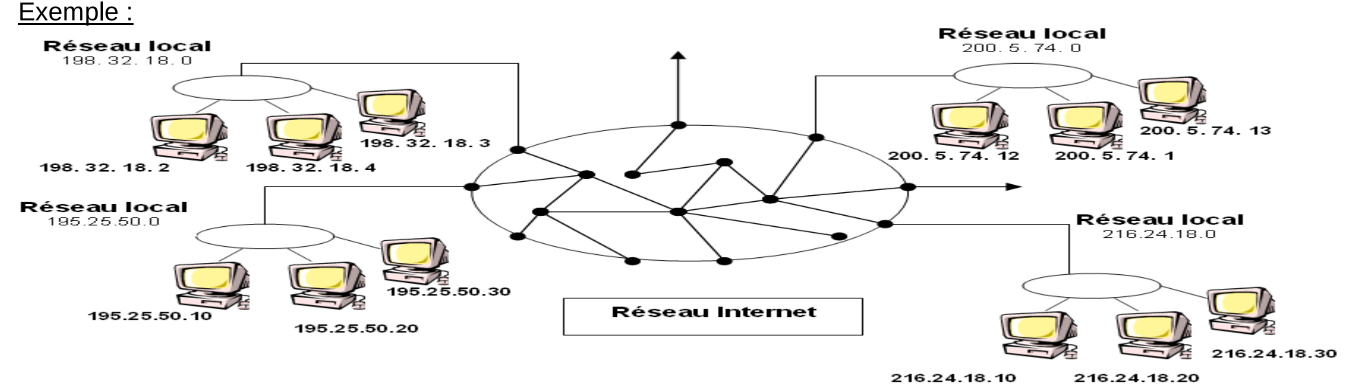
F . Adressage du réseau IPv4

1. Introduction :

Chaque point de connexion, ou interface, d'un équipement dispose d'une adresse IP associée à un réseau. Cette @ permet à d'autres ordinateurs de localiser cet équipement sur un réseau spécifique.
Une adresse IP est une séquence de 32 bits composée de 1 et de 0, Afin de faciliter leur lecture, les adresses IP sont généralement exprimées sous la forme de quatre nombres décimaux séparés par des points.

@ IP = 32 bits = $(8bits)_{10}$. $(8bits)_{10}$. $(8bits)_{10}$. $(8bits)_{10}$

Exemple :



2. Adressage IPv4 et masque associé à la classe :

Un routeur utilise l'adresse IP du réseau de destination afin de remettre le paquet au réseau approprié. On parle dans ce cas de système d'adressage hiérarchique, car il contient plusieurs niveaux de sous réseaux.
A chaque adresse IP est associé un masque de sous-réseau, ou netmask, qui est constitué de 32 bits.
Chaque adresse IP regroupe deux identificateurs différents :

- la première partie identifie l'adresse réseau «network number» représentée sur le masque par les <11>.
- la seconde, identifie la machine sur le réseau «host number» représentée sur le masque par les <00>.

@ IP = <network number> <host number>
Masque = <111111111111111><00000000000>

Les adresses IP sont réparties en ***classes*** afin de définir des réseaux de différentes tailles :
- Les adresses de classe ***A*** sont affectées aux réseaux de grande taille.
- Les adresses de classe ***B*** sont utilisées pour les réseaux de taille moyenne
- Les adresses de classe ***C*** pour les réseaux de petite taille.

Classe	Plage d'adresses du premier octet	Bits de poids Fort de l'@ IP	Masque associé à la classe	Nombre de bits de l'adresse réseau	Plage des @ IP privées ou locales non routables
A	De 0 à 127	0	255. 0. 0. 0	8	De 10.0.0.0 à 10.255.255.255
B	De 128 à 191	10	255. 255. 0. 0	16	De 172.16.0.0 à 172.31.0.0
C	De192 à 223	110	255. 255. 255. 0	24	De 192.168.0.0 à 192.168.255.255
D	De 224 à 239	1110	255. 255. 255. 224	28	Non définie
E	De 240 à 255	11110	Non définit	Non définit	Non définie

- Seules les classes A, B et C sont utilisées pour adresser les PC d'un réseau IP.
- Les adresses de classe D est réservée à la diffusion multicast d'une adresse IP.
- Les adresses de classe E est réservés à des fins expérimentales par le groupe IETF (*Internet Engineering Task Force*)

Adresses IP réservées ou non valides pour un PC :

Les adresses suivantes sont réservées : non valides et non utilisables par un PC.
- Le réseau 127.0.0.0 est réservé pour les tests en bouclage.
- ***Une adresse réseau*** : adresse IP dont tous les ***bits hôte*** sont occupés par des ***0*** binaires est réservée pour identifier l'adresse réseau.
- ***Une adresse de broadcast*** : une adresse IP dont tous les ***bits hôte*** sont occupés par des ***1*** binaires est réservée pour l'adresse de Broadcast(diffusion des paquets vers tous les les équipements du réseau.

Adresses IP publiques et privées :

À l'origine, un organisme portant le nom d'***InterNIC*** (*Internet Network Information Center*) était chargé de la vérification de l'unicité des adresses IP. Celui-ci n'existe plus et a été remplacé par l'***IANA*** (*Internet Assigned Numbers Authority*).

- Chaque adresse IP publique étant unique, deux ordinateurs connectés à un réseau public ne peuvent pas avoir la même adresse IP publique.
- Les adresses IP publiques sont payantes obtenues auprès d'un Fournisseur d'Accès Internet (FAI).

Pour résoudre le problème de pénurie (manque) d'adresses IP publiques plusieurs solutions sont utilisées :

- élaboration du routage CIDR (*Classless interdomain routing*)
- élaboration de la norme IPv6.
- utilisation des adresses privées.

La connexion d'un réseau à Internet par le biais d'adresses publiques nécessite la conversion des adresses privées en adresses publiques. Ce processus de conversion est appelé «***NAT***» (*Network Address Translation*).

3. Utilité du masque de sous-réseau

A l'aide d'une adresse IP et du masque de sous-réseau, on peut définir :

- L'adresse réseau associée,
- La partie hôte associée,
- L'adresse de diffusion associée qui désigne tous les hôtes de ce réseau.
- La plage des adresses IP valides sur ce réseau

❖ Un « ET » logique appliqué entre le masque de réseau et l'adresse IP permet d'obtenir l'adresse d'un réseau correspondant.

- Calcul de l'adresse réseau en binaire

@ IP	1100 0001	1111 1100	0001 0011	0000 0011
Masque Réseau	1111 1111	1111 1111	1111 1111	0000 0000
@ Réseau	1100 0001	1111 1100	0001 0011	0000 0000

- Calcul de l'adresse réseau en décimal

@ IP	193	252	19	3
Masque Réseau	255	255	255	0
@ Réseau	193	252	19	0

❖ Un « ET » logique appliqué entre le complément à 1 du masque de réseau et une adresse IP permet d'obtenir la partie hôte correspondante.

- Calcul de l'adresse hôte en binaire

@ IP	1100 0001	1111 1100	0001 0011	0000 0011
Masque Réseau	0000 0000	0000 0000	0000 0000	1111 1111
@ Hôte	0000 0000	0000 0000	0000 0000	0000 0011

- Calcul de l'adresse hôte en décimal

@ IP	193	252	19	3
Masque Réseau	0	0	0	255
@ Hôte	0	0	0	3

❖ Le tableau suivant fournit ces informations pour trois adresses IP prises parmi les trois classes fondamentales.

Adresse IP	10. 25. 2. 5	172. 17. 5. 8	192. 168. 53. 24
Classe	A	B	C
Masque de réseau	255. 0. 0. 0	255. 255. 0. 0	255. 255. 255. 0
Adresse de réseau	10. 0. 0. 0	172. 17. 0. 0	192. 168. 53. 0
Adresse de diffusion	10. 255. 255. 255	172. 17. 255. 255	192. 168. 53. 255
Complément à 1 du masque	0.255.255.255	0.0.255.255	0.0.0.255
Partie hôte de l'adresse	0.25.2.5	0.0.5.8	0.0.0.24
Plage des adresses IP du réseau	De : 10. 0. 0. 1 A : 10. 255. 255. 254	De : 172. 17. 0. 1 A : 172. 17. 255. 254	De : 192. 168. 53. 1 A : 192. 168. 53. 254

4. Notion de sous-réseau

Le découpage d'un réseau en sous-réseaux implique l'utilisation du masque de sous réseau afin de fragmenter un réseau de grande taille en segments (ou sous-réseaux) plus petits, plus faciles à gérer et plus efficaces.
Pour créer une adresse de sous-réseau, l’administrateur réseau emprunte des bits du champ d’hôte et les désigne comme champ de sous-réseau.

n bits s bits h bits

@ IP = <network number><subnet number><host number>
Masque = <1111111111111111111111111111111><00000000000>

n+s bits à 1 h bits à 0
n+s+h = 32 bits

- n=8, 16 ou 24 selon la classe
- s permet de créer 2^s sous-réseaux différents
- h permet de définir 2^h-2 adresses IP valides dans chaque sous-réseau

Exemple n°1 :

Un réseau d'adresse 160.16.0.0 est divisé en 4 sous-réseaux. Chacun de ces 4 sous-réseaux accueille moins de 254 hôtes.
Adresse de classe B donc n=16 donc s+h=16 : nous disposons de 16 bits pour les numéros de sous-réseau et les numéros d'hôtes. Dans ce cas, on peut choisir la solution simple qui consiste à prendre 8 bits pour le numéro de sous-réseau, et 8 bits pour le numéro d'hôte. Ce choix permet d'adresser 256 sous-réseaux et 254 hôtes par sous-réseau. On cherche toujours à maximiser le nombre de sous-réseaux disponibles.
Le masque de sous-réseau s'obtient en positionnant les bits de réseau et de sous-réseau à 1 et les bits d'hôtes à 0. Ceci donne en binaire :

11111111	11111111	11111111	00000000
réseau		sous réseau	hôte

Soit en représentation décimale : 255.255.255.0
Les adresses de sous-réseaux sont obtenues en listant toutes les possibilités sur les bits de sous-réseaux, et en positionnant les bits d'hôte à 0. Les adresses de sous-réseaux et les adresses d'hôtes seront :

Liste des sous-réseaux	Numéros de sous-réseaux	Adresses de sous-réseau	Adresses d'hôte
Sous réseau 0	0	160.16.0.0	160.16.0.1 à 160.16.0.254
Sous réseau 1	1	160.16.1.0	160.16.1.1 à 160.16.1.254
Sous réseau 2	2	160.16.2.0	160.16.2.1 à 160.16.2.254
Sous réseau 3	3	160.16.3.0	160.16.3.1 à 160.16.3.254
Sous réseau 4	4	160.16.4.0	160.16.4.1 à 160.16.4.254
...	...	...	... à ...
Sous réseau 254	254	160.16.254.0	160.16.254.1 à 160.16.254.254
Sous réseau 255	255	160.16.255.0	160.16.255.1 à 160.16.255.254

Exemple n°2

Le même réseau d'adresse 160.16.0.0 est divisé en 8 sous-réseaux. Les sous-réseaux ont au plus 3000 hôtes.
Le masque précédent ne convient plus. Pour adresser 8 sous-réseaux différents, il faut 8 numéros. 3 bits permettent d'adresser 6 (8-2) sous-réseaux et 4 bits permettent d'adresser 14 sous-réseaux. Il faut donc prendre cette dernière solution. Il reste dans ce cas, 12 bits pour le numéro d'hôte ce qui permet 4094 numéros d'hôtes ce qui convient parfaitement. Le masque sera donc :

11111111	11111111	11110000	00000000
réseau		sous réseau	hôte

Soit en représentation décimale : 255.255.240.0
Pour déterminer les numéros de sous-réseaux, il faut toujours lister les possibilités sur 4 bits, en tenant compte des poids. Ceci nous donne :

0000 (0000)	soit 0	0100 (0000)	soit 64	1000 (0000)	soit 128	1100 (0000)	soit 192
0001 (0000)	soit 16	0101 (0000)	soit 80	1001 (0000)	soit 144	1101 (0000)	soit 208
0010 (0000)	soit 32	0110 (0000)	soit 96	1010 (0000)	soit 160	1110 (0000)	soit 224
0011 (0000)	soit 48	0111 (0000)	soit 112	1011 (0000)	soit 176	1111 (0000)	soit 240

5. Comparaison entre IPv4 et IPv6 :

Dans les années 80, la stratégie d'adressage proposée par la version IPv4 s'avérait relativement évolutive. Néanmoins, elle ne réussit pas à satisfaire les exigences liées à l'attribution des adresses.

Les adresses de classe A et B représentent 75% de l'espace d'adresses IPv4. Toutefois, moins de 17 000 organisations peuvent recevoir un numéro de réseau de classe A ou B.
Le nombre d'adresses réseau de classe C est nettement plus important que celui des adresses de classe A et B, bien qu'il ne représente que 12,5 % des quatre milliards d'adresses IP disponibles.

Dès 1992, le groupe IETF (Internet Engineering Task Force) a identifié deux problèmes :
· La diminution inquiétante des adresses réseau IPv4 disponibles.
· La hausse importante et rapide du volume des tables de routage d'Internet.
IPv6 encode les adresses sur ***128 bits*** au lieu de 32 (en utilisant des nombres hexadécimaux). La représentation abrégée IPv6 consiste en huit nombres de 16 bits séparés par ':', chaque nombre de 16 bits est représenté par quatre chiffres hexadécimaux.

Exemple 2001:0DB8:AC10:FE01:0000:0000:0000:0000 = 2001:0DB8:AC10:FE01::

Calcul du nombre d'adresses IPv6 par mm^2 de la surface de la terre :

Le nombre d'adresses disponibles est de 2^{128} soit $3,4 \times 10^{38}$

Le rayon de la terre, qu'on assimilera à une sphère, est d'environ 6 360 km.

La surface de la terre est donc de : $4 \times PI \times r^2 = 4 \times 3,14 \times 6\,360 \times 6360 = 508 \,.\, 10^6 \; km^2$
soit $508 \,.\, 10^6 \times 10^{12} = 508 \times 10^{18} \; mm^2$

Le nombre d'adresses IP disponibles par mm^2 de la surface terrestre est donc de :
$3,4 \times 10^{38} \; / \; 508 \times 10^{12} = 669 \times 10^{15}$

Nous disposerons donc de plus de 600 millions de milliards d'adresses par mm^2

6. Obtention d'une adresse Internet :

Un hôte réseau doit se procurer une adresse unique mondialement afin de se connecter à Internet. Le routeur n'utilise pas l'adresse MAC pour transmettre des données au-delà du réseau local.
Les administrateurs réseau font appel à deux méthodes différentes pour affecter les adresses IP. Il s'agit des méthodes **statique** et **dynamique**.

6.1. Adressage statique :

L'attribution statique convient particulièrement aux réseaux de petite taille qui subissent peu de changements. L'administrateur système effectue manuellement les opérations d'affectation et de suivi des adresses IP pour chaque hôte.
Les serveurs, les imprimantes et les routeurs doivent être obligatoirement doté d'une adresse statique.

6.2. Attribution d'une adresse IP à l'aide du protocole RARP

Le protocole ***RARP*** associe des adresses MAC connues à des adresses IP.
Le protocole RARP permet à l'équipement de lancer une requête afin de connaître son adresse IP (dans le cas d'une station sans disque dur par exemple).
Les requêtes RARP sont diffusées sur le LAN et c'est le serveur RARP, habituellement un routeur, qui y répond.

6.3. Attribution d'une adresse IP à l'aide du protocole BOOTP

Le protocole ***BOOTP*** *(Bootstrap Protocol)* fonctionne dans un environnement client serveur et ne requiert qu'un seul échange de paquet pour obtenir des informations sur le protocole IP (@IP, @routeur, @serveur …).
Le protocole BOOTP permet à un administrateur réseau de créer un fichier de configuration qui définit les paramètres de chaque équipement. L'administrateur doit ajouter les hôtes et tenir à jour la base de données.
BOOTP utilise la couche UDP pour transporter les messages.
Lorsqu'un client envoie un message BOOTP, le serveur BOOTP lui répond.

6.4. Gestion des adresses IP à l'aide du protocole DHCP

Le protocole ***DHCP*** *(Dynamic Host Configuration Protocol)* a été proposé pour succéder au protocole BOOTP. Contrairement au protocole BOOTP, le protocole DHCP permet à un hôte d'obtenir une adresse IP de *manière dynamique* sans que l'administrateur réseau ait à définir un profil pour chaque équipement. Avec le protocole DHCP, il suffit qu'une plage d'adresses IP soit définie.
Le protocole DHCP dispose d'un avantage majeur sur le protocole BOOTP, car il permet aux utilisateurs d'être mobiles.

7. VLSM et CIDR.

7.1. Introduction

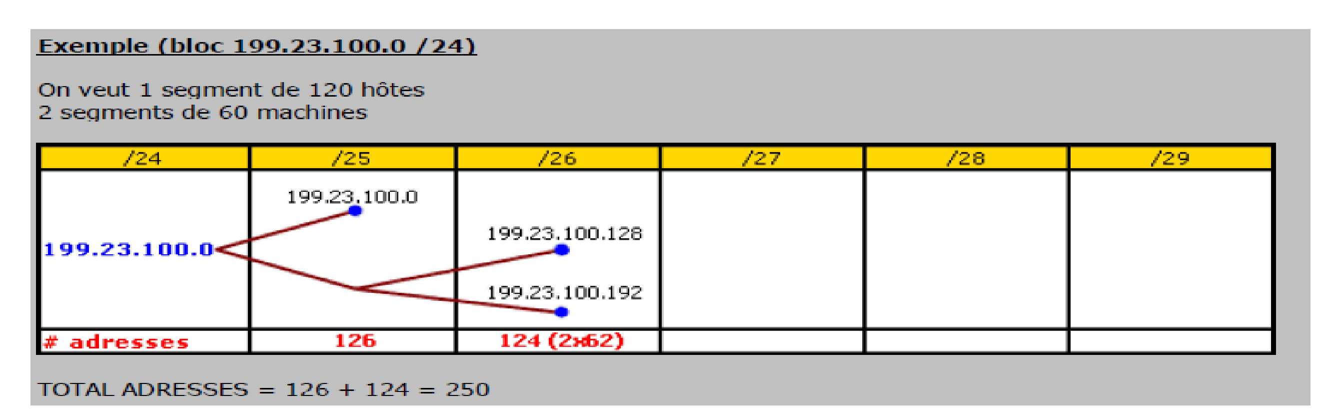
VLSM (Variable-lenght subnet masking) a été développé pour permettre de multiplier les niveaux de subnet au sein d'un même réseau, c'est à dire que le masque de réseau ne reste pas figé.
Cela permet donc d'utiliser plusieurs masques de sous réseaux dans le même réseau.
En quelques sortes, "on subnette un subnet", ce qui va augmenter l'efficacité d'adressage et va permettre de "résumer les routes" (route summarization)
VLSM est en quelques sortes une extension de CIDR (Classless Inter-Domain Routing) .
Ces deux notions sont en fait étroitement liées, la seule différence est que VLSM est destiné à un réseau interne propre à une organisation, tandis que CIDR lui peut agir dans le réseau internet (mondial).
IL existe des protocoles (fonctionnant en classless) qui supportent le VLSM et des protocoles (fonctionnant en classful) qui ne le supportent pas.

7.2. Exemple n°1 :

Vous êtes chargé de planifier l'adressage de différents petits LANs. Vous utilisez la technique du VLSM afin d'obtenir les résultats requis en terme d'hôtes.

- **Lors de divisions successives de blocs d'adresses, conservez toujours les blocs supérieurs et divisez le dernier bloc.**
- **Indiquez les numéros de réseau en notation CIDR et schématisez les divisions des blocs.**
- **Indiquez le nombre d'adresses valides par segment ainsi que le nombre global d'adresses valides.**

Exemple (bloc 199.23.100.0 /24) On veut 1 segment de 120 hôtes 2 segments de 60 machines TOTAL ADRESSES = 126 + 124 = 250



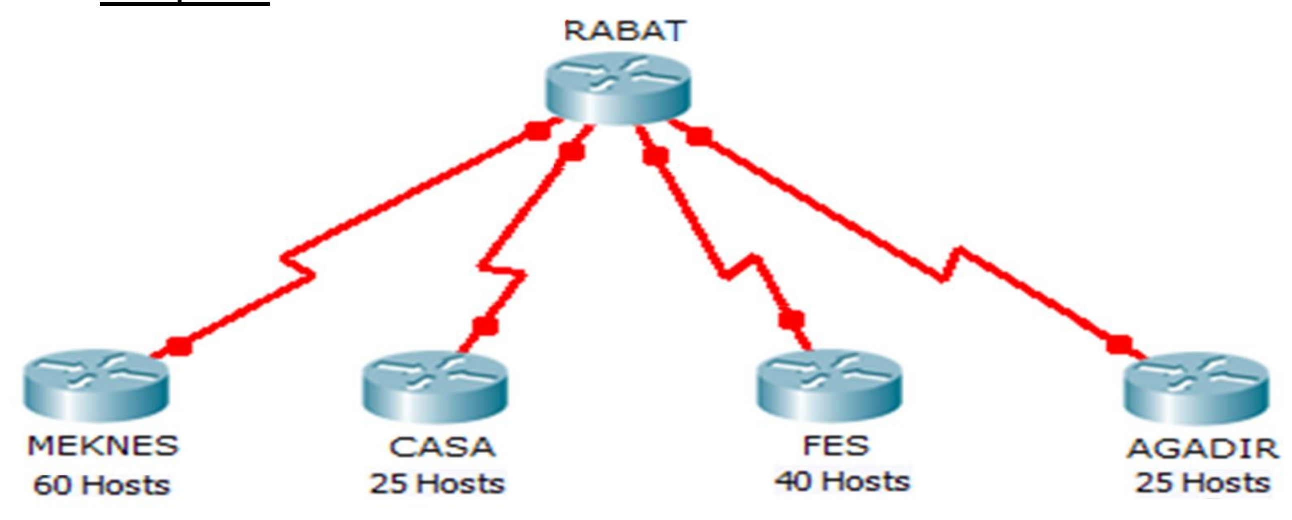
Exemple (bloc 199.23.100.0 /24)

On veut 1 segment de 120 hôtes
2 segments de 60 machines

/24	/25	/26	/27	/28	/29
199.23.100.0	199.23.100.0	199.23.100.128 199.23.100.192			
# adresses	126	124 (2x62)			

TOTAL ADRESSES = 126 + 124 = 250

7.3. Exemple n°2



Pour l'adresse réseau suivante : 192.124.16.0/21
1- Etablir un plan d'adressage ***VLSM*** en respectant les besoins :

- Le *Réseau* MEKNES: 60 hôtes.
- Le Réseau CASA: 25 hôtes.
- Le Réseau FES: 40 hôtes.
- Le Réseau AGADIR: 25 hôtes.
- Liaison WAN: 4.

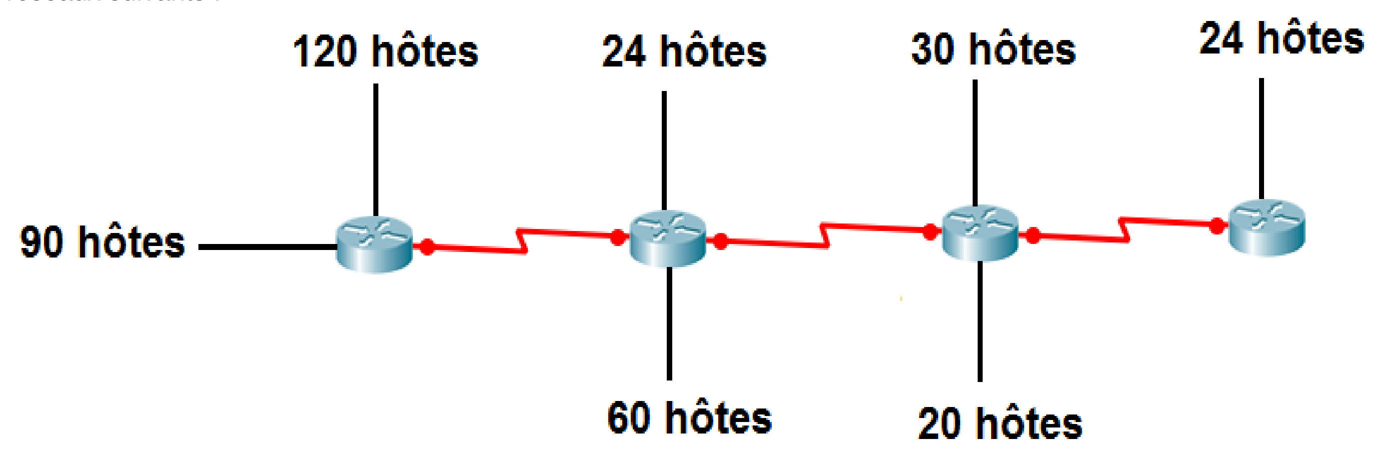
2- Masque de chaque réseau.
3- La plage de chaque réseau.
4- Adresse de diffusion (broadcast) de chaque réseau.

La solution :

Réseau	TAILLE	Adresse réseau	Masque	Plage	diffusion
Meknes	60	192.124.16.0	/26	192.124.16.1 à 192.124.16.62	192.124.16.63
Fes	40	192.124.16.64	/26	192.124.16.65 à 192.124.16.126	192.124.16.127
Agadir	25	192.124.16.128	/27	192.124.16.129 à 192.124.16.158	192.124.16.159
Casa	25	192.124.16.160	/27	192.124.16.161 à 192.124.16.190	192.124.16.191
WAN1	2	192.124.16.192	/30	192.124.16.193 à 192.124.16.194	192.124.16.195
WAN2	2	192.124.16.196	/30	192.124.16.197 à 192.124.16.198	192.124.16.199
WAN3	2	192.124.16.200	/30	192.124.16.201 à 192.124.16.202	192.124.16.203
WAN4	2	192.124.16.204	/30	192.124.16.205 à 192.124.16.206	192.124.16.207

7.4. Exemple n°3

A partir de l'adresse réseau 192.168.30.0/23 construire un adressage VLSM respectant la taille des sous-réseaux suivants :



Solution de l'exemple :

a. LAN 1 —120 hôtes : 192.168.30.0/25 (2^7 = 128 - 2 = 126 hôtes de 192.168.30.1 à 192.168.30.126)

b. LAN 2—90 hôtes : 192.168.30.128/25 (2^7 = 128 - 2 = 126 hôtes de 192.168.30.129 à 192.168.30.254)

c. LAN 3—60 hôtes : 192.168.31.0/26 (2^6 = 64 - 2 = 62 hôtes de 192.168.31.1 à 192.168.31.62)

d. LAN 4—24 hôtes : 192.168.31.64/27 (2^5 = 32 - 2 = 30 hôtes de 192.168.31.65 à 192.168.31.94)

e. LAN 5—30 hôtes : 192.168.31.96/27 (2^5 = 32 - 2 = 30 hôtes de 192.168.31.97 à 192.168.31.126)

f. LAN 6—20 hôtes : 192.168.31.128/27 (2^5 = 32 - 2 = 30 hôtes de 192.168.31.129 à 192.168.31.158)

g. LAN 7—24 hôtes : 192.168.31.160/27 (2^5 = 32 - 2 = 30 hôtes de 192.168.31.161 à 192.168.31.190)

Il est possible d'attribuer les éléments suivants aux liaisons série :

a. 192.168.31.192/30 avec les adresses hôte 192.168.31.193 et 192.168.31.194

b. 192.168.31.196/30 avec les adresses hôte 192.168.31.197 et 192.168.31.198

c. 192.168.31.200/30 avec les adresses hôte 192.168.31.201 et 192.168.31.202

REMARQUE:
Les adresses attribuées aux interfaces série ont été sélectionnées à l'extrémité de la plage d'adresses affectées aux LAN au cours de l'étape 3. Cela laisse libre la plage d'adresses de 192.168.31.204 à 192.168.31.255

7.5 Exercice n°1 sur la technique du découpage VLSM :

Vous êtes chargé de planifier l'adressage de différents petits LANs. Vous utilisez la technique du VLSM afin d'obtenir les résultats requis en termes d'hôtes. Lors de divisions successives de blocs d'adresses, conservez toujours les blocs supérieurs et divisez le dernier bloc.

- Vérifier s'il est possible de faire un découpage sans VLSM.
- Indiquez les numéros de réseau en notation CIDR et schématisez les divisions des blocs. Indiquez le nombre d'adresses valides par segment ainsi que le nombre global d'adresses valides.
- Schématiser ce découpage sous forme de cercle.

Premier réseau (bloc 195.220.12.0 /24)
1 segment d'au moins 115 postes
1 segment d'au moins 58 postes
1 segment d'au moins 25 machines
1 segment d'une douzaine d'hôtes
2 segments pour des groupes de travail de 5 machines

/24	/25	/26	/27	/28	/29
195.220.12.0					
# adresses					

Second réseau (bloc 192.168.10.0 /24)
3 segments d'une soixantaine d'hôtes
1 segment d'une trentaine de postes
1 segment d'au moins 11 machines

/24	/25	/26	/27	/28	/29
192.168.10.0					
# adresses					

Troisième réseau (bloc 222.8.15.0 /24)
1 segment de 100 machines
4 segment dde 28 hôtes minimum

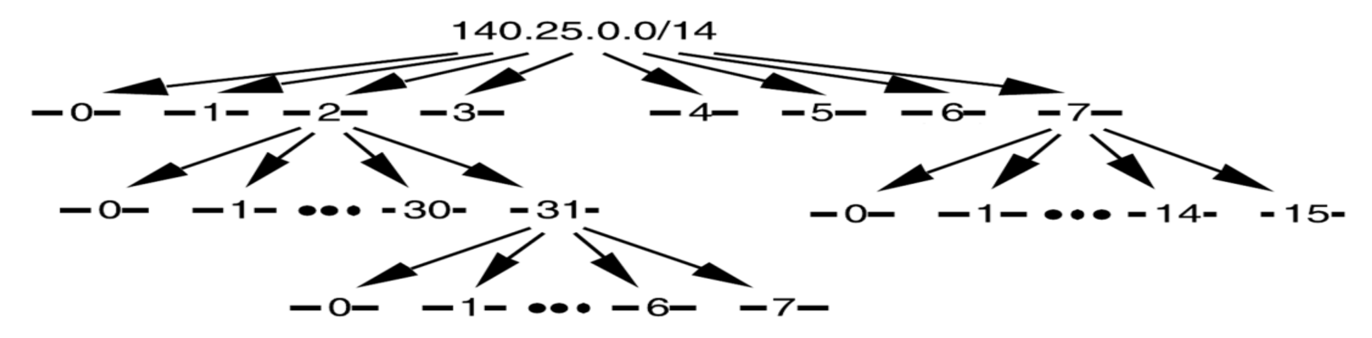
/24	/25	/26	/27	/28	/29
222.8.15.0					
# adresses					

Quatrième réseau (bloc 200.157.115.0 /24)
1 segment de 120 postes
3 segments de 30 postes
2 segments de 12 postes

/24	/25	/26	/27	/28	/29
200.157.115.0					
# adresses					

Exercice n°2

On attribue le réseau 140.25.0.0/14 et on étudie le déploiement de sous-réseaux avec des masques réseau de longueur variable ou Variable Length Subnet Mask (VLSM). Voici le schéma de découpage de ces sous-réseaux.



1. Quelle est la liste des adresses des 8 sous-réseaux issus du découpage de premier niveau ?
2. Quelle est la plage des adresses utilisables pour le sous-réseau numéro 3 ?
3. Quelle est la liste des adresses des 16 sous-réseaux obtenus à partir du sous-réseau numéro 7?
4. Quelle est la plage des adresses utilisables pour le sous-réseau numéro 7 - 14 ?
5. Quelle est l'adresse de diffusion du sous-réseau numéro 7 - 7 ?
6. Quelle est la plage des adresses utilisables pour le sous-réseau numéro 2 - 31 - 2 ?
7. Quelle est l'adresse de diffusion du sous-réseau numéro 2 - 31 - 5 ?

G . Couche liaison de données

I. Technologies de la couche accès réseau (liaison de données + physique):

Au niveau de la couche accès réseau on trouve plusieurs technologies ADSL, ETHERNET, Token Ring et RNIS.

1. Technologies WAN

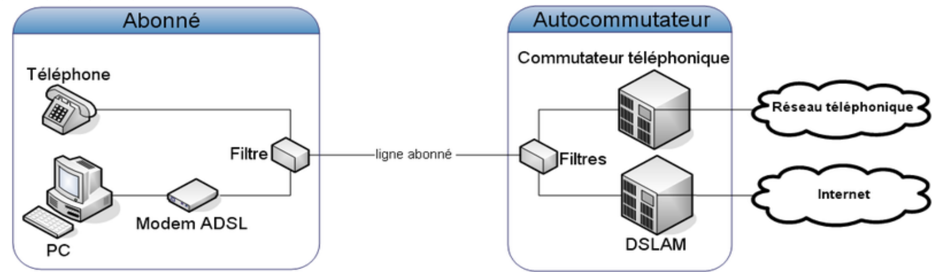
a. RNIS

On peut voir l'architecture RNIS comme une évolution entièrement numérique des réseaux téléphoniques existants, conçue pour associer la voix, les données, la vidéo et toute autre application ou service. RNIS s'oppose donc au réseau téléphonique commuté (RTC) traditionnel.

b. ADSL (Asymmetric Digital Subscriber Line**)**

Le sigle anglais ADSL signifie Asymmetric Digital Subscriber Line, qui se traduit fonctionnellement par « [liaison] numérique [à débit] asymétrique [sur] ligne d'abonné ». La terminologie française officielle recommande l'expression « liaison numérique asymétrique », mais le sigle « ADSL » reste le plus largement utilisé dans le langage courant.

Comme son nom l'indique, la technologie ADSL fournit un débit asymétrique. Le flux de données est plus important dans un sens de transmission que dans l'autre. Contrairement à la technologie SDSL pour laquelle le débit est symétrique, donc équivalent en émission et en réception, le débit de données montant d'une communication ADSL (upload) est plus faible que le débit descendant (download), dans un rapport qui varie généralement entre 5 et 20.



2. Technologies LAN

On distingue les trois technologies LAN usuelles suivantes :

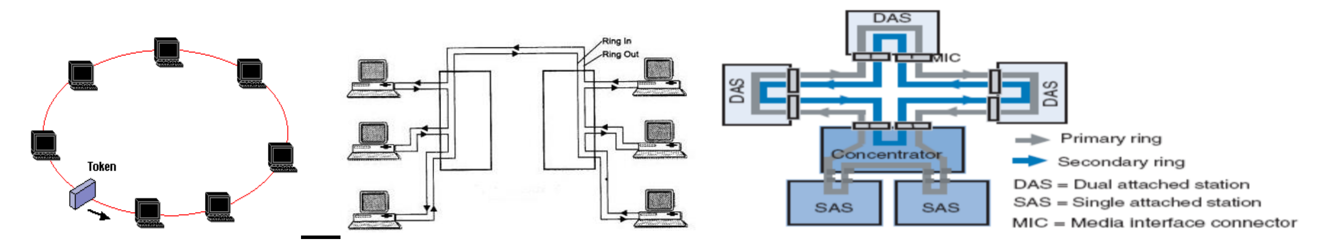


a. Réseau local de type Ethernet

Ethernet est un protocole de réseau local à commutation de paquets. L'Ethernet est basé sur le principe de membres (pairs) sur le réseau, envoyant des messages dans un canal commun, parfois appelé l'éther. Chaque pair est identifié par une clé globalement unique, appelée adresse MAC, pour s'assurer que tous les postes sur un réseau Ethernet aient des adresses distinctes. Une technologie connue sous le nom de Carrier Sense Multiple Access with Collision Detection (Écoute de porteuse avec accès multiples et détection de collision) ou CSMA/CD régit la façon dont les postes accèdent au média.

b. Réseau local Token Ring

L'Anneau à jeton, plus connu internationalement sous le terme de Token Ring, est un réseau local qui fonctionne sur la couche Liaison du modèle OSI dont l'architecture de base est un anneau physique et logique. L'apparition des MAU a permis de se libérer d'une topologie physique en anneau, puisque le câblage s'est alors effectué en étoile. *Il existe plusieurs normes à jeton passant. Sur des topologies en anneau (IEEE 802.5, Token Ring ou FDDI) mais aussi sur des topologies en bus (IEEE 802.4).*



II. Méthodes d'accès au support

Sur un canal point à point un émetteur peut transmettre librement. En revanche, lorsque le support est partagé par plusieurs périphériques, il est nécessaire de gérer la façon dont les données sont échangées.

Elles dépendent de l'architecture réseau, c'est-à-dire de la topologie logique. Suivant le cas, le signal sera diffusé sur le support et atteindra les bornes de chaque carte réseau ou transitera de poste en poste en étant répété par chaque station.

Une méthode d'accès décrit les règles qui régissent l'accès, la transmission et la libération du canal partagé. On distingue essentiellement trois types de méthodes : la contention, le jeton passant et le polling.

1. Contention

Avec la contention, chaque station émet quand elle le veut, après écoute du canal (Carrier Sense ou écoute de la porteuse), qui doit être disponible. La trame émise est écoutée, pour vérifier qu'aucun autre signal ne vient perturber l'émission. Il n'existe dans ce cas aucun arbitrage du canal. Bien qu'écoutant le support partagé, deux stations peuvent émettre simultanément ce qui conduit à une sur-tension (en coaxial) ou à une réception d'informations sur la paire émettrice (en paire torsadée) : dans ce cas, on parle d'une collision.

Le plus important, dans cette méthode, est qu'une station émettrice soit capable de déterminer si sa trame est ou non entrée en collision avec une autre.

Les deux implémentations les plus répandues pour la contention sont CSMA/CD et CSMA/CA.
CSMA correspond à l'écoute de la porteuse (Carrier Sense) sur un support partagé (Multiple Access). Les deux mises en oeuvre se distinguent par le fait que l'une détecte les collisions (Collision Détection), et l'autre tente de les éviter (Collision Avoidance). Dans ce dernier cas, plutôt que d'essayer de transmettre les données en risquant une collision (après écoute du support), le périphérique va envoyer une trame préliminaire pour avertir les autres stations qu'elle veut prendre possession du canal (pour envoyer sa trame de données).
CSMA/CD correspond à l'implémentation Ethernet, tandis que CSMA/CA est celle adoptée par LocalTalk (réseaux Macintosh) et Le WIFI.

Avantages et Inconvénients

Le gros avantage de cette gestion du canal est sa simplicité. Cependant, la méthode n'est pas déterministe, car le temps d'accès au canal n'est pas prévisible. De plus aucune gestion de priorité n'est possible pour des matériels qui ont des besoins d'accéder rapidement au support partagé.

2. Jeton passant

Dans la méthode du jeton passant on utilise la topologie physique en anneau, les trames circulent de poste en poste, chacun se comportant comme un répéteur. Initialement, une petite trame (le jeton) est répétée de poste en poste jusqu'à ce qu'une machine qui désire émettre le conserve pendant un temps fixé.
Le jeton est un message d'autorisation qui donne le contrôle du canal à la station qui le possède. La station détentrice du jeton peut émettre sa trame, qui va être répétée par chaque station et faire ainsi le tour de l'anneau. Au passage, le destinataire de la trame qui voit passer le signal en fait une copie (si celle-ci n'est pas erronée et si le récepteur dispose de suffisamment de place dans son tampon de réception). La trame qui a été copiée est marquée par le destinataire pour informer l'émetteur que la trame a ou non été lue. Une fois que la trame a fait le tour de l'anneau, l'émetteur retire sa trame et retransmet le jeton vers la prochaine station.

Avantages et inconvénients

Le jeton passant implémente une solution déterministe qui permet un bon contrôle du canal.
Le débit maximum réel atteint est beaucoup plus élevé qu'en Ethernet qui est sujet aux collisions.

Jeton passant contre contention

La contention est meilleure sur les réseaux à faible charge, car dans ce cas, il n'y a que très peu de collisions. On a déterminé que 11% de collisions constituait un maximum à ne pas dépasser.
Au contraire, le jeton passant nécessite tout un mécanisme de gestion du canal, ce qui le rend meilleur lorsque la charge réseau est élevée.

3. Polling

Un matériel est désigné comme administrateur de l'accès au canal. Ce matériel, le maître, interroge dans un ordre prédéterminé chacun des autres matériels et leur demande s'ils ont des informations à transmettre. Le plus souvent, le maître est un concentrateur et les matériels secondaires sont les nœuds de l'étoile.

Avantages et Inconvénients

L'avantage est que tous les accès au canal sont centralisés. De plus, le temps d'accès et le volume des données manipulées sur le canal sont prévisibles et fixés.
Cependant, la méthode utilise une partie de la bande passante du réseau pour émettre des messages d'avertissement et des acquittements.
On peut citer comme exemple de polling, la méthode d'accès de priorité à la demande (ou DPAM, Demand Priority Access Method) gérée par la norme 100VG AnyLan.

H . Ethernet

1. Définition d'un réseau Ethernet

Ethernet est la technologie LAN la plus répandue. Le groupe DIX (Digital, Intel et Xerox) a été le premier à la mettre en œuvre. DIX a créé et mis en œuvre la première spécification LAN Ethernet, qui a servi de base à l'élaboration de la norme 802.3 de l'IEEE (Institute of Electrical and Electronics Engineers) introduite en 1980. L'IEEE a étendu la norme 802.3 à trois nouveaux comités : 802.3u pour Fast Ethernet, 802.3z pour Gigabit Ethernet sur fibre optique et 802.3ab pour Gigabit Ethernet sur câble à paires torsadées non blindées.

La figure suivante présente les différentes versions d'Ethernet.

liaison de données Couche
physique Couche
IEEE 802.2
Ethernet
10BASE2
10BASE5
10BASE-T
10BASE-F
100BASE-TX
100BASE-FX
1000BASE-T
Norme Digital, Intel Xerox (DIX)
Spécifications 802.3 pour 10 Mbits/s Ethernet
802.3u Spécifications pour 100 Mbits/s (Fast) Ethernet
802.3z Spécifications pour 1000 Mbits/s (Gigabit) Ethernet

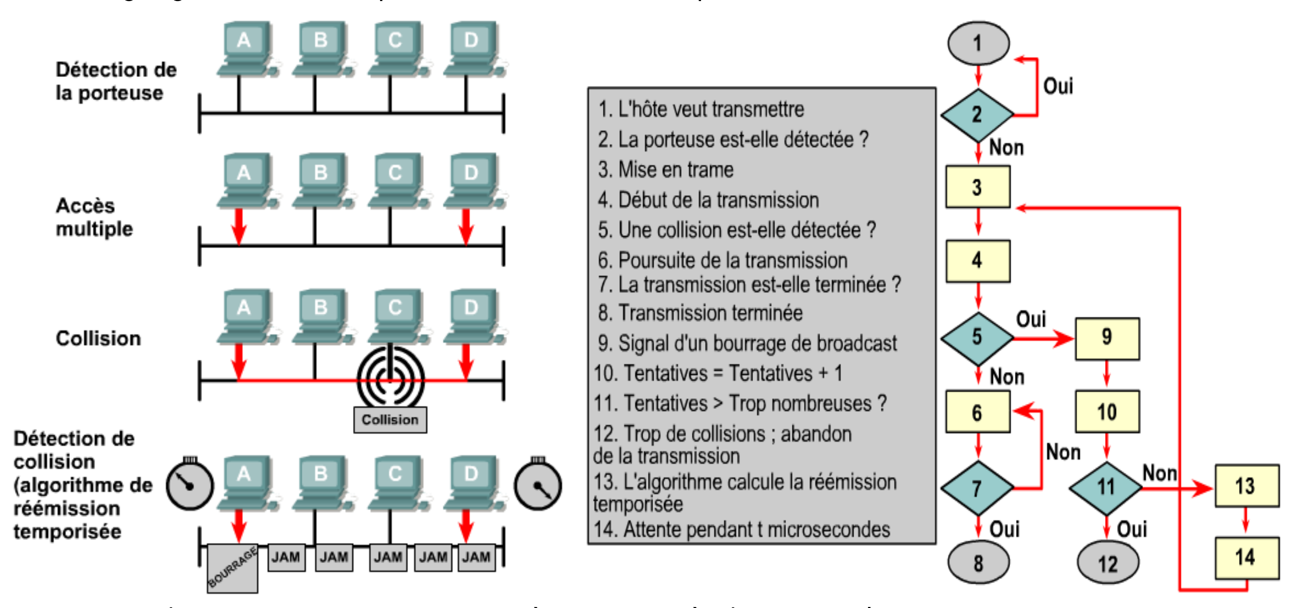
Le tableau suivant donne les domaines d'utilisation des différentes technologies Ethernet.

	Mise en œuvre Ethernet 10BaseT	Mise en œuvre Fast Ethernet	Mise en œuvre Gigabit Ethernet
Niveau utilisateur final (de l'équipement utilisateur final vers l'équipement	Permet une connectivité pour les applications de petite taille et de taille	Permet un accès à 100-Mbits/s au serveur pour les stations de travail hautes performances.	Généralement pas utilisé à ce niveau.
Niveau groupe de travail (de l'équipement groupe de travail au backbone)	Généralement pas utilisé à ce niveau.	Permet la connectivité entre l'utilisateur final et les groupes de travail. Permet la connectivité du groupe de travail au backbone. Permet la connectivité du bloc serveur à la couche backbone.	Permet une connectivité hautes performances au bloc serveur de l'entreprise.
Niveau backbone	Généralement pas utilisé à ce niveau.	Permet la connectivité du bloc serveur groupe de travail au backbone.	Permet une connectivité haut débit pour l'équipement du réseau et le backbone.

2. Protocole Ethernet

Ethernet repose sur un algorithme d'accès multiple CSMA/CD, signifiant Carrier Sense Multiple Access with Collision Detection C'est un protocole permettant la discussion sur un réseau de type Ethernet.

Voici l'organigramme de description du fonctionnement du protocole de discussion CSMA/CD :



- Les adaptateurs peuvent commencer à transmettre à n'importe quel moment
- Les adaptateurs ne transmettent jamais lorsqu'ils détectent une activité sur le canal
- Les adaptateurs interrompent leur transmission dès qu'ils détectent l'activité d'un autre adaptateur au sein du canal (détection de collisions)
- Avant de procéder à la retransmission d'une trame, les adaptateurs patientent pendant une durée aléatoire relativement courte.

3. Caractéristiques des différentes technologies Ethernet

Le tableau ci-dessous compare les spécifications de câbles et de connecteurs relatives aux implémentations des différentes normes Ethernet.

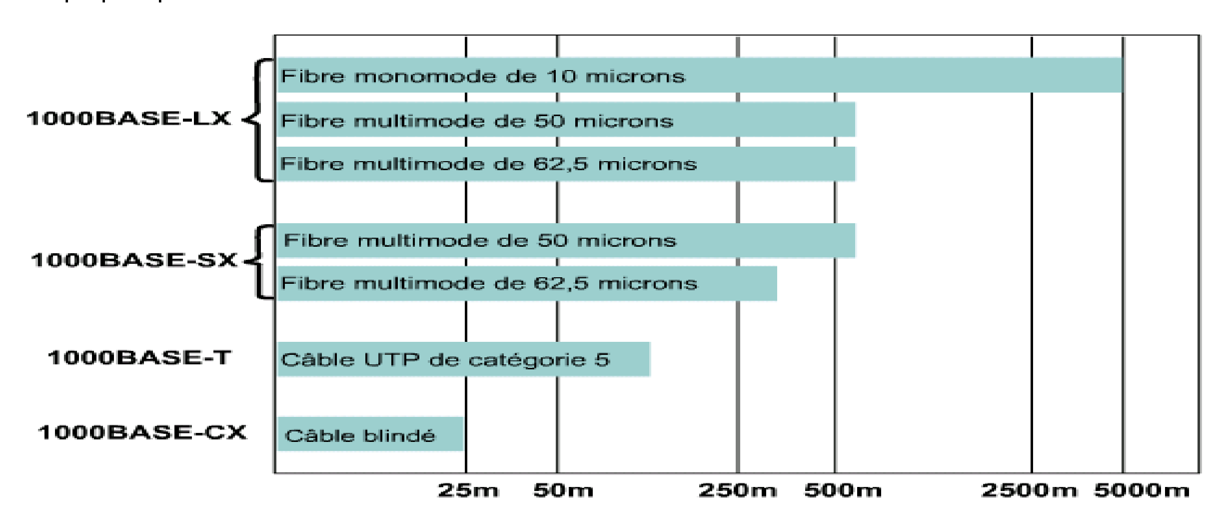
	10BASE2	10BASE5	10BASE-T	100BASE-TX	100BASE-FX	1000BASE-CX	1000BASE-T	1000BASE-SX	1000BASE-LX
Médias	Câble coaxial de 50 ohms (Ethernet à câble fin)	Câble coaxial de 50 ohms (Ethernet épais)	Câble EIA/TIA Catégorie 3, 4, 5 UTP, deux paires	Câble EIA/TIA Catégorie 5 UTP, deux paires	Fibre multimode de 62,5/125	STP	Câble EIA/TIA catégorie 5 UTP, quatre paires	Fibre multimode de 62,5/50 microns.	Fibre multimode de 62,5/50 microns ; fibre monomode de 9 microns.
Longueur maximale du segment	185 m	500 m	100 m	100 m	400 m	25 m	100 m	275 m pour la fibre de 62,5 microns ; 550 m pour la fibre de 50 microns	440 m pour la fibre de 62,5 microns ; 550 m pour la fibre de 50 microns ; de 3 à 10 km pour la fibre monomode.
Topologie	En bus	En bus	En étoile	En éto	En étoile	En étoile	En étoile	En étoile	En étoile
Connecteur	BNC	AUI (Attachment Unit Interface)	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)	Connecteur d'interface média duplex Connecteur ST ou SC	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)	Connecteur SC	Connecteur SC

Ethernet est une technologie dont la vitesse a été multipliée par 1 000, de 10 à 10 000 Mbits/s, en moins d'une décennie. Toutes les versions d'Ethernet présentent une structure de trame similaire, permettant une excellente interopérabilité. La plupart des connexions en cuivre Ethernet sont désormais en mode full duplex commuté, et la technologie Ethernet avec câblage en cuivre la plus rapide est 1000BASE-T, ou Gigabit Ethernet. La technologie 10 Gigabit Ethernet et les versions plus rapides utilisent essentiellement des fibres optiques.

a. Les technologies Ethernet 10BASE5, 10BASE2 et 10BASE-T sont considérées comme les versions initiales d'Ethernet ; Ces versions n'existent plus maintenant.

b. La technologie Ethernet 100 Mbits/s, ou Fast Ethernet, peut être mise en œuvre à l'aide d'un fil en cuivre à paires torsadées (100BASE-TX, par exemple) ou avec un média à fibre optique (100BASE-FX, par exemple).
   - Les réseaux Ethernet 100 Mbits/s peuvent offrir un débit de 200 Mbits/s en mode full duplex.
   - La longueur sans répéteur est toujours de 100 m.

c. La technologie Gigabit Ethernet avec un câblage en cuivre est mise en œuvre de la façon suivante :
   - Un câblage UTP de catégorie 5e et des améliorations électroniques prudentes permettent de passer d'un débit de 100 à 125 Mbits/s par paire de fils.
   - Les quatre paires de fils sont utilisées, et pas seulement deux d'entre elles. On obtient ainsi débit de 4 fois 125 Mbits/s, soit 500 Mbits/s pour les quatre paires de fils.
   - Des composants électroniques sophistiqués autorisent les collisions permanentes sur chaque paire de fil en mode full duplex, doublant ainsi le débit (de 500 à 1 000 Mbits/s).
   - Les versions à fibre optique des systèmes Gigabit Ethernet, 1000BASE-SX et 1000BASE-LX présentent les avantages suivants : elles ne génèrent pas de bruit, leur taille est réduite, elles permettent de disposer de bandes passantes plus larges et elles autorisent des distances non répétées plus grandes. La norme IEEE 802.3 recommande d'utiliser la norme Gigabit Ethernet sur des fibres optiques pour le backbone.



d. La norme 10 Gigabit Ethernet (IEEE 802.3ae) a été élaborée en juin 2002.
- Il s'agit d'un protocole en mode full duplex qui utilise uniquement la fibre optique comme support de transmission.
- La distance maximale de transmission dépend du type de fibre utilisé. Avec les fibres monomodes, cette distance est de 40 km.
- Au fur et à mesure des discussions entre les membres IEEE, on commence à envisager la possibilité d'une création de normes pour les technologies 40, 80 et même 100 Gigabit Ethernet.

Mise en œuvre	Longueur d'onde	Média	Bande passante modale minimale	Longueur d'exploita
10GBASE-LX4	1310 nm	62.5µm MMF	500 MHz/km	2 - 300 m
10GBASE-LX4	1310 nm	50µm MMF	400 MHz/km	2 - 240 m
10GBASE-LX4	1310 nm	50µm MMF	500 MHz/km	2 - 300 m
10GBASE-LX4	1310 nm	10µm MMF	N/A	2 - 10 km
10GBASE-S	850 nm	62.5µm MMF	160 MHz/km	2 - 26 m
10GBASE-S	850 nm	62.5µm MMF	200 MHz/km	2 - 33 m
10GBASE-S	850 nm	50µm MMF	400 MHz/km	2 - 66 m
10GBASE-S	850 nm	50µm MMF	500 MHz/km	2 - 82 m
10GBASE-S	850 nm	50µm MMF	2000 MHz/km	2 - 300 m
10GBASE-L	1310 nm	10µm SMF	N/A	2 - 10 km
10GBASE-E	1550 nm	10µm SMF	N/A	2 - 30 km

4. Structure d'une trame Ethernet

La figure suivante illustre les différents champs d'une trame Ethernet

Trame Ethernet							
Préambule	SFD	Destination	Source	Type de longueur	Données	Bourrage	FCS
7	1	6	6	2	De 46 à 1 500		4

Préambule : Ce champ est codé sur 7 octets et permet de synchroniser l'envoi. Chacun des octets vaut 10101010 et cette série permet à la carte réceptrice de synchroniser son horloge.

SFD : Ce champ est codé sur 1 octet et indique à la carte réceptrice que le début de la trame va commencer. La valeur de SFD (Starting Frame Delimiter) est 10101011.

Adresse destination : Ce champ est codé sur 6 octets et représente l'adresse MAC (Medium Access Control) de l'adaptateur destinataire. Dans le cadre d'un broadcast, l'adresse utilisée est FF-FF-FF-FF-FF-FF.
Cette adresse est ce que l'on appelle l'adresse physique d'une carte Ethernet (Hardware address). En fait cette adresse est divisée en deux parties égales :
- Les trois premiers octets désignent le constructeur. C'est le l'organisation OUI (Organizationally Unique Identifier) gérer par l'IEEE, qui référence ces correspondances.
- Les trois derniers octets désignent le numéro d'identifiant de la carte, dont la valeur est laissée à l'initiative du constructeur qui possède le préfixe

L'association de l'IEEE et du constructeur assure ainsi l'unicité de l'attribution des numéros d'adresse MAC.

Adresse source : Ce champ est codé sur 6 octets et représente l'adresse MAC (Medium Access Control) de l'adaptateur émetteur.

Ether Type : Ce champ est codé sur 2 octets et indique le type de protocole inséré dans le champ donnée. Voici un extrait des différentes correspondances :

0x6000 - DEC	0x0600 - XNS	0x0806 - ARP	0x8035 - RARP	0x8100 - 802.1Q
0x0609 - DEC	0x0800 - IPv4	0x8019 - Domain	0x809B - AppleTalk	0x86DD - IPv6

Données : Ce champ est codé entre 46 et 1500 octets et contient les données de la couche 3. Dans le cas de TCP/IP, c'est ici que vient se loger le datagramme IP. L'unité de transfert maximale est le MTU (Maximale Transfer Unit) et sa valeur est classiquement de 1500 octets. Si la taille des données est inférieure à 46 octets, alors elle devra être complétée avec des octets de bourrage (padding) et c'est la couche réseau qui sera chargée de les éliminer.

FCS : Ce champ est codé sur 4 octets et représente la séquence de contrôle de trame. Il permet à l'adaptateur qui réceptionnera cette trame de détecter toute erreur pouvant s'être glissée au sein de la trame.
Les erreurs binaires sont principalement créées par les variations d'affaiblissement du signal et l'induction électromagnétique parasite dans les câbles Ethernet ou les cartes d'interface. La valeur de FCS (Frame Check Sequence) est le résultat d'un calcul polynomial appelé CRC (Cyclic Redundancy Code). A la réception de la trame, la couche liaison effectue le même calcul et compare les deux résultats qui doivent être égaux afin de valider la conformité de la trame reçue.

5. Exemple de structure d'une trame Ethernet

```
AA AA AA AA AA AA AA AB
08 00 20 0A 70 66 08 00
20 0A AC 96 08 00 45 00
00 28 A6 F5 00 00 1A 06
75 94 C0 5D 02 01 84 E3
3D 05 00 15 0F 87 9C CB
7E 01 27 E3 EA 01 50 12
10 00 DF 3D 00 00 20 20
20 20 20 20 9B 52 46 43
```

```
--------------------------- début d'une trame Ethernet ---------------------------------------------------
AA AA AA AA AA AA AA AB      -> Synchronisation
08 00 20 0A 70 66            -> @mac destinataire (constructeur = 080020)
08 00 20 0A AC 96            -> @mac émetteur (même constructeur)
08 00                        -> Type (ici IP). Si < à 1500 c'est une longueur
--------------------------- 46 <= contenu (ici datagramme IP)<= 1500 ------------------------------------
4                            -> Version IP (Ipv4)
5                            -> Longueur de l'en-tête (5*32bit = 160bit ou 5*4 octets = 20 octets)
00 00 28 A6 F5 00 00  1A   06   75 94 C0 5D 02 01 84 E3 3D 05 -> en tête
 |   |___|  |___|  |___|  |_|  |_|  |____| |__________| |___________|
 |    |      |      |      |    |     |         |                  |_ @IP destinataire 132.227.61.5 classe B
 |    |      |      |      |    |     |         |_ @IP émetteur 192.93.2.1 classe C [pas dans le même réseau !]
 |    |      |      |      |    |     |_Bloc de contôle d'erreur (sur l'en-tête du datagramme seulement)
 |    |      |      |      |    |_ Protocole (ici TCP)
 |    |      |      |      |_ TTL (ici 1A = 1*16+10=26 routeurs ou secondes)
 |    |      |      |_ Drapeau + Déplacement (0=inutl, 0=DF(fragmentation autorisée) 0=MF (pas de fragments à
suivre, donc dernier fragment) 0000000000000=déplacement soit place du 1er octet transporté, ici 1er fragment)
[Il s'agit d'un datagramme non fragmenté]
 |    |      |_Id du datagramme (numéro quelconque, ne sert que si le datagramme est amené à être fragmenté )
 |    |_ Longueur totale (ici 28 en hexadécimal vaut 2*16=8 en décimal soit 40 octets)
 |_ pas de qualité de service
--------------------------- contenu = segment TCP d'une longueur de 20 octets (40-20) --------------------------
00 15                        -> port source, ici 21 donc serveur ftp
0F 87                        -> port destination 3975, port quelconque du client
9C CB 7E 01                  -> Numéro de séquence (n° du 1er octet transporté émis (tiré au hasard))
27 E3 EA 01                  -> Numéro de séquence (n° du 1er octet attendu en réception)
5                            -> Longueur de l'en-tête du segment (20 octets) :
                             on peut donc en déduire que ce segment ne contient pas de données
0 12 = 0000 0001 0010        -> Drapeaux (ici réponse 'ok' d'ouverture de connexion)
       |_____|||  ||||_FIN (Clôture de la connexion)
          |   ||  |||_SYN (Ouverture (ou réponse d'ouverture) de connexion)
          |   ||  ||_RST (réinitialisation de la connexion)
          |   ||  |_PSH (Livraison immédiate)
          |   ||_ACK (accusé de réception)
          |   |_URG (urgent)
          |_6 bits réservés
10 00                        -> Taille de la fenêtre, ici 4096 octets. Quantité de données que l'émetteur
                             est autorisé à envoyer sans accusé de réception
DF 3D                        -> BCE (Bloc de contrôle d'erreur sur le segment entier)
00 00                        -> Pointeur vers les données urgentes (inutile ici puisqu'il n'y a pas de
                             données urgents bit URG =0)
--------------------------- fin du segement TCP (sans données) -------------------------------------------------
--------------------------- fin des données du datagramme IP --------------------------
20 20 20 20 20 20            -> 6 octets de bourrage pour amener la trame Ethernet à la
                             longueur MINIMALE autorisée
9B 52 46 43                  -> Bloc de contôle d'erreur de la trame Ethernet
--------------------------- fin de la trame Ethernet ---------------------------------------------------
```

7. Exemple de méthode de calcul du CRC (FCS)

Méthode de calcul du CRC

– Calcul d'un checksum basé sur l'arithmétique polynomiale modulo 2
– On considère le mot binaire suivant de taille *n :* b=(bn-1,bn-2,...,b1,b0)
– Ce mot s'exprime sous la forme d'un polynôme de degrés n-1, à coefficients binaire :

$$B(X)=b_{n-1}.X^{n-1} + b_{n-2}.X^{n-2} + ... + b_1.X + b_0$$

– La clé C(X) associée à un tel mot est définie comme étant le reste de la division de $B(X).X^k$ par un polynôme générateur G(X) de degré k.
– Le mot à transmettre est alors $M(X) = B(X).X^k + C(X)$.

Exemple d'utilisation des CRCs

– CRC-1 (bit de parité) : $G(X) = X + 1$
– CRC-8 (ATM) : $G(X) = X^8 + X^2 + X + 1$
– CRC-16 (USB, PPP, Bluetooth, ...)
– CRC-32 (Ethernet) : $G(X) = X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + X + 1$
– CRC-160 (MD5 checksum)

Question : Quelle est la clé associée au mot 110111 avec $G(X) = X^2+X+1$?

– Mot = 110111
– $B(X) = X^5 + X^4 + X^2 + X + 1$
– $B(X).X^2 = X^7 + X^6 + X^4 + X^3 + X^2$
- Calcul : $B(X).X^2 / G(X) = ...$

$B(X).X^2 = X^7 + X^6 + X^4 + X^3 + X^2$	$G(X) = X^2 + X + 1$
$-(X^7 + X^6 + X^5)$	$P(X) = X^5 + X^3 + 1$
$X^5 + X^4 + X^3 + X^2$	
$-(X^5 + X^4 + X^3)$	
X^2	
$-(X^2 + X + 1)$	
$C(X) = X + 1$	

En algèbre binaire (modulo 2), on a : 1+1 = 0 ou encore 1 = -1, par conséquent ajouter est identique à soustraire !

– Le reste est $C(X) = X+1$
– Donc la clé est 11 (coefficients de C(X))

– Le mot à envoyer sera 110111**11**

Question : Comment peut-on détecter une erreur ?

- M(X) est le polynôme correspondant au mot transmis...
– M(X) doit être divisible par G(X).
– On peut le vérifier en effectuant la division de M(X) par G(X) ; le reste R(X) doit être nul.
– Si ce n'est pas le cas, une erreur est détectée !

Question : Quelle condition doit vérifier B(X), C(X) et G(X) ?

– $B(X).X^k = P(X).G(X) + C(X)$ avec C(X) de d° < k
– $M(X) = B(X).X^k + C(X) = P(X).G(X) + C(X) + C(X) = P(X).G(X)$

I . Couche physique OSI

La couche physique OSI fournit le moyen de transporter sur le support réseau les bits constituant une trame de couche liaison de données. Cette couche accepte une trame complète de la couche liaison de données et la code sous la forme d’une série de signaux transmis sur le support local. Les bits codés composant une trame sont reçus par un périphérique final ou intermédiaire.

La transmission de trames sur le support local exige les éléments de couche physique suivants :

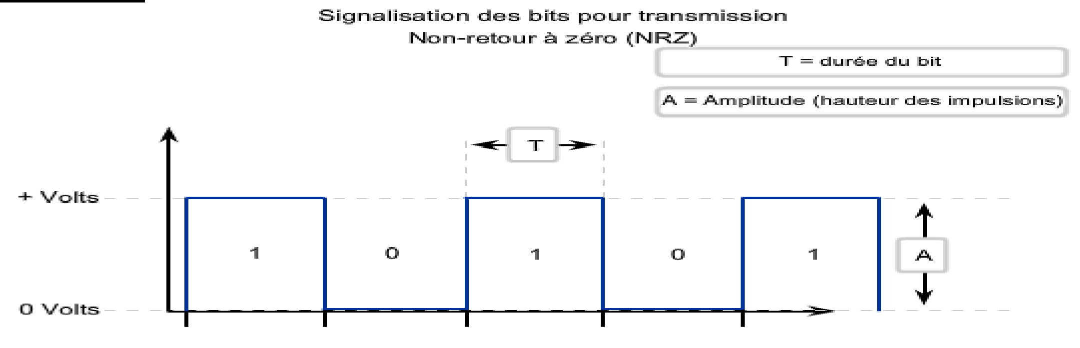
- le support physique et les connecteurs associés,
- une représentation des bits sur le support,
- le codage de données et des informations de contrôle,
- l’ensemble de circuits émetteur et récepteur sur les périphériques réseau.

L’objectif de la couche physique est de créer le signal électrique, optique ou micro-ondes qui représente les bits dans chaque trame. Ces signaux sont alors envoyés sur le support individuellement

I . Signalisation et codage physique : représentation de bits

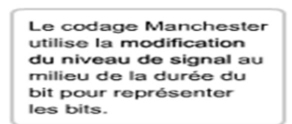
La couche physique représente chacun des bits de la trame sous la forme d’un signal. Chaque signal placé sur le support dispose d’un temps spécifique d’occupation du support. On parle de durée du bit. Les signaux sont traités par le périphérique de réception, qui rétablit leur représentation binaire.
La méthode de signalisation utilisée doit être compatible avec une norme pour que le récepteur puisse détecter les signaux et les décoder. La norme contient un accord entre l’émetteur et le récepteur sur la manière de représenter des 1 et des 0. En l’absence d’accord de signalisation (c’est-à-dire si différentes normes sont utilisées à chaque extrémité de la transmission), la communication sur le support physique échoue.

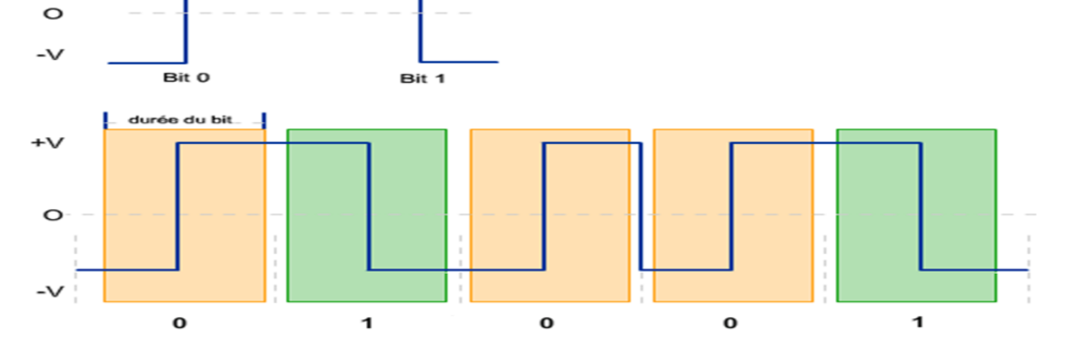
1 . Signalisation NRZ



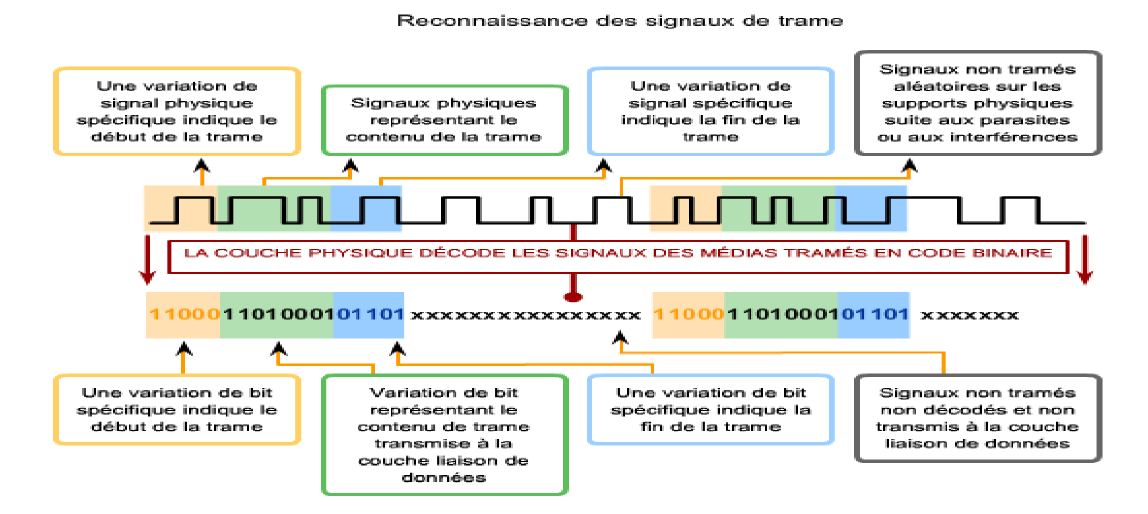
2 . Codage Manchester

Signalisation des bits pour transmission
Codage Manchester





3 . Codage et regroupement des codes



II . Caractéristiques des supports de transmissions

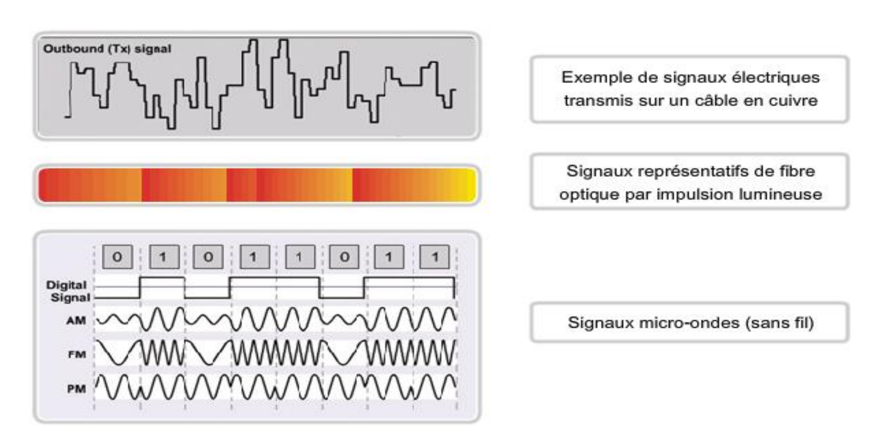
1. Définition des supports de transmission des données

Les supports physiques de transmissions sont les éléments permettant de faire circuler les informations entre les équipements de transmission. On classe généralement ces supports ou canaux en trois catégories, selon le type de grandeur physique qu'ils permettent de faire circuler, donc de leur constitution physique :

- Les **supports filaires** permettent de faire circuler une grandeur électrique sur un câble généralement métallique (Câble de cuivre)
- Les **supports optiques** permettent d'acheminer des informations sous forme lumineuse
- Les **supports aériens** désignent l'air ou le vide, ils permettent la circulation d'ondes électromagnétiques ou radioélectriques diverses

Selon le type de support physique, la grandeur physique a une vitesse de propagation plus ou moins proche de la vitesse de la lumière qui a une célérité C= 300 000 km/s.

Exemple de représentation des signaux sur les supports physiques :

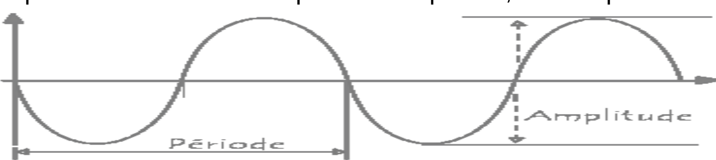


2. Notions sur les ondes électromagnétiques

La transmission de données sur un support physique se fait par propagation d'un phénomène vibratoire. Il en résulte un signal ondulatoire dépendant de la grandeur physique que l'on fait varier :

- dans le cas de la lumière il s'agit d'une onde lumineuse
- dans le cas du son il s'agit d'une onde acoustique
- dans le cas de la tension ou de l'intensité d'un courant électrique il s'agit d'une onde électrique...

Les ondes électromagnétiques sont caractérisées par leur fréquence, leur amplitude et leur phase.



3. Notion sur les perturbations

La transmission de données sur une ligne ne se fait pas sans pertes. Tout d'abord le temps de transmission n'est pas immédiat, ce qui impose une certaine "synchronisation" des données à la réception.
D'autre part des parasites ou des dégradations du signal peuvent apparaître.

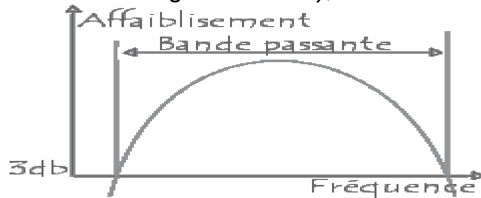
- **Les parasites** (souvent appelés *bruit*) sont l'ensemble des perturbations modifiant localement la forme du signal. On distingue généralement trois types de bruit :
- **Le bruit blanc** est une perturbation uniforme du signal, c'est-à-dire qu'il rajoute au signal une petite amplitude dont la moyenne sur le signal est nulle. Le bruit blanc est généralement caractérisé par un ratio appelé ***rapport signal/bruit***, qui traduit le pourcentage d'amplitude du signal par rapport au bruit (son unité est le décibel). Celui-ci doit être le plus élevé possible.
- **Les bruits impulsifs** sont de petits pics d'intensité provoquant des erreurs de transmission.
- **L'affaiblissement** du signal représente la perte de signal en énergie dissipée dans la ligne. L'affaiblissement se traduit par un signal de sortie plus faible que le signal d'entrée et est caractérisée par la valeur:

  A = 10 log (Niveau du signal en sortie / Niveau du signal en entrée) Niveau en puissance

  L'affaiblissement est proportionnel à la longueur de la voie de transmission et à la fréquence du signal.
- **La distorsion** du signal caractérise le déphasage entre le signal en entrée et le signal en sortie.

4. Bande passante et capacité

- La **bande passante** (en anglais *bandwidth*) d'une voie de transmission est l'intervalle de fréquence sur lequel le signal ne subit pas un affaiblissement supérieur à une certaine valeur (généralement 3 dB, car 3 décibels correspondent à un affaiblissement du signal de 50%), on a donc :



Une ligne de téléphone a par exemple une bande passante comprise entre 300 et 3400 Hertz environ pour un taux d'affaiblissement égal à 3 dB.

- La **capacité** d'une voie est la quantité d'informations (en bits) pouvant être transmis sur la voie en 1 seconde.

La capacité se caractérise de la façon suivante :

$$C = W \log_2 (1 + S/N)$$

C capacité (en bps)
W la largeur de bande (en Hz)
S/N représente le rapport signal sur bruit de la voie.

5. Débit applicatif et débit réel ou en ligne

Débit applicatif < Débit en ligne < bande passante pour différentes raisons, telles que le mécanisme d'encapsulation, le type de données transmises, les équipements d'inter-réseau, la topologie de réseau, le nombre d'utilisateurs sur le réseau et le serveur.

Durée idéale = Taille / Bande Passante et
Durée réelle = (Taille+encapsulations) / Débit en ligne = Taille / Débit applicatif.

6. Numérique et analogique.

- La majorité des transmissions sont effectuées par le biais d'ondes électromagnétiques. Ces transmissions sont dites analogiques si les informations transportées par ces ondes sont de nature continue (forme physique de la voix et de la vidéo par exemple).
- Dans la signalisation numérique, toutes les informations sont envoyées sous forme de bits. La voix, la vidéo et les données sont converties en flux de bits lors de leur préparation pour une transmission via des médias numériques.

7. Upload et download

On appelle download le téléchargement en mode descendant (du serveur vers votre ordinateur) et on appelle upload le téléchargement en mode ascendant (de votre ordinateur vers le serveur). Il est intéressant de savoir que l'upload et le download se font sur des canaux de transmissions séparés (que ce soit sur un modem ou une ligne spécialisée). Ainsi lorsque vous envoyez un document (upload) vous ne perdez pas de bande passante en download !

8. Rapidité de modulation

On peut tout de suite différencier la notion de rapidité de modulation **R** (exprimée en baud) de celle de débit binaire **D** (exprimée en bit/s).

La rapidité de modulation **R** correspond au nombre d'éléments (symboles) transmis sur le canal par seconde ; elle est différente du débit binaire **D** dès que l'on associe plus d'un seul élément binaire (bit) à un même symbole transmis. La relation entre la rapidité de modulation **R** et le débit binaire **D** met en jeu la valence **V**; elle est donnée par l'équation :

$$D = R \log_2 (V)$$

La valence **V** est le nombre d'états distincts (symboles) présents sur le signal de transmission.

Par exemple, on peut décider d'associer à chaque groupe de 2 bits à transmettre une tension (symbole) définie par le tableau suivant

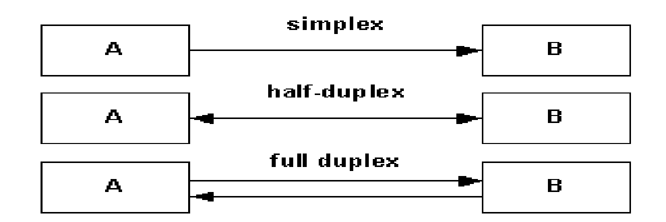
0 0	-5 V
0 1	-2,5 V
1 1	2,5V
1 0	5V

On définit ainsi un code à plusieurs niveaux, dit code M-aire (ici quaternaire).
Ici, sur la ligne on va trouver 4 états différents (4 symboles) : la valence est donc **V= 4**. La relation entre le débit binaire **D** et la rapidité de modulation est $D = R \log_2 (4) = 2.R$

La rapidité de modulation est donc deux fois plus faible que le débit binaire. Si on veut transmettre des bits à raison de 1200 bit/s en utilisant cette technique, on obtiendra une rapidité de modulation de 600 bauds.

9. Modes de liaison

Mode simplex : La transmission ne peut se faire que de A vers B (ex : radio, télévision)
Mode semi-duplex : La transmission peut se faire dans les deux sens, mais pas en même temps (ex : CB, talkie-walkie).
Mode duplex intégral : La transmission peut se faire dans les deux sens simultanément (ex : téléphone)



III . Exemples de caractéristiques des principaux supports de transmission.

Types de médias	Bande passante théorique	Distance théorique maximale
Câble coaxial de 50 ohms (Ethernet 10Base2 ; Ethernet à câble fin)	10 Mbits/s	185 m
Câble coaxial de 50 ohms (Ethernet 10Base5 ; câble Ethernet épais)	10 Mbits/s	500 m
Paire torsadée non blindée (UTP) de catégorie 5 (UTP) (Ethernet 10BaseT)	10 Mbits/s	100 m
Paire torsadée non blindée (UTP) de catégorie 5 (UTP) (Ethernet 100BaseTX)	100 Mbits/s	100 m
Paire torsadée non blindée (UTP) de catégorie 5 (UTP) (Ethernet 1000BaseTX)	1000 Mbits/s	100 m
Fibre optique multimode (62,5/125 m) (Ethernet 100BaseFX)	100 Mbits/s	220 m
Fibre optique multimode (62,5/125 m) (Ethernet 100BaseFX)	1000 Mbits/s	220 m
Fibre optique multimode (50/125 m) (Ethernet 1000BaseSX)	1000 Mbits/s	550 m
Fibre optique monomode (9/125 m) (Ethernet 1000BaseLX)	1000 Mbits/s	5000 m

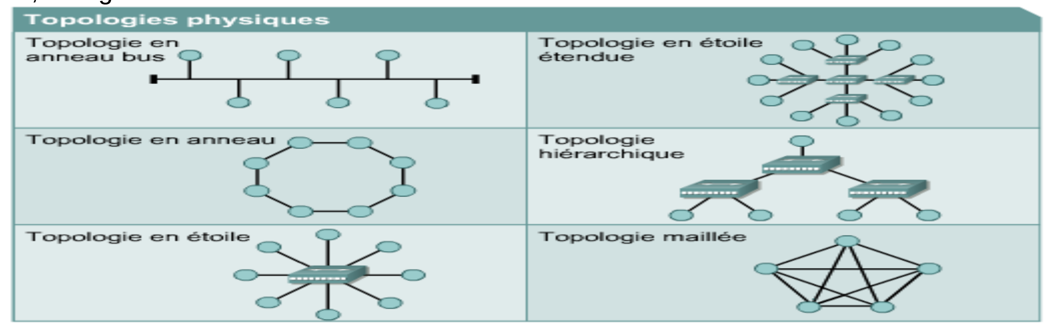
J . Planification et câblage des réseaux

I . Introduction

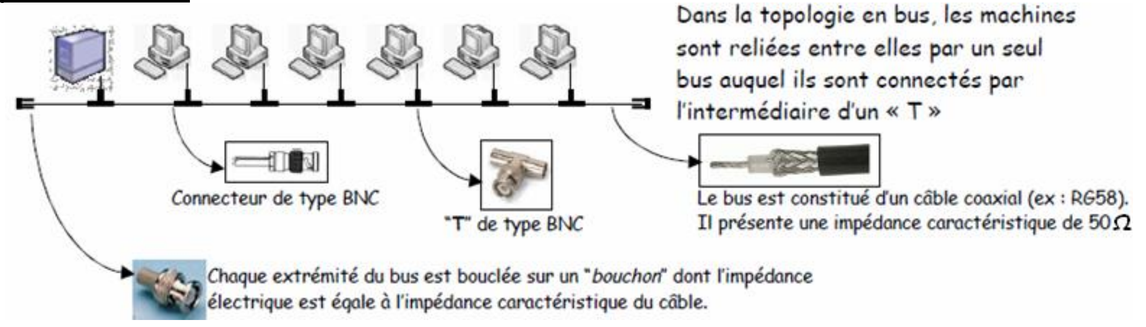
Un réseau local est un réseau informatique de taille géographique restreinte. Il peut concerner, par exemple, une salle informatique, une habitation particulière, un bâtiment, un établissement scolaire, une entreprise …
Couramment appelé LAN (Local Area Network) il peut également être nommé RLE (Réseau Local d'Entreprise)
Le réseau permet d'interconnecter, dans un rayon limité, plusieurs types de terminaux (postes de travail informatiques, serveurs, caisse enregistreuses, imprimantes …)
L'objectif est de faire communiquer les divers équipements dans le but de partager des données et des services (logiciels, accès Internet, impressions, gestion à distance …)
Les réseaux peuvent être de divers types mais c'est le réseau Ethernet qui s'impose aujourd'hui grâce à sa simplicité de mise en oeuvre et à l'augmentation progressive des débits de connexion
(10 Mb/s, puis 100 Mb/s, 1 Gb/s voir 10 Gb/s aujourd'hui)

II . Architectures : topologies physiques

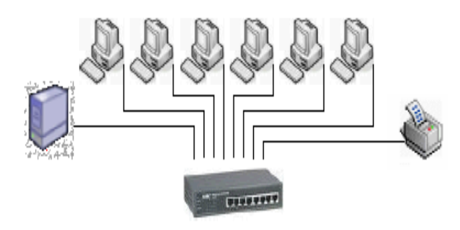
Une topologie caractérise la façon dont les différents équipements réseaux sont positionnés les uns par rapport aux autres.
On distinguera en plus, la topologie physique (par rapport au plan du réseau) de la topologie logique (qui précise davantage la façon dont les informations circulent au plus bas niveau).
Il est très important de bien différencier ces deux aspects. Par exemple, un concentrateur pourra être vu d'un point de vue logique, comme un anneau en Token Ring (ce concentrateur étant alors un MAU), alors que physiquement, il s'agit d'une connexion en étoile.



2.1. Topologie en bus

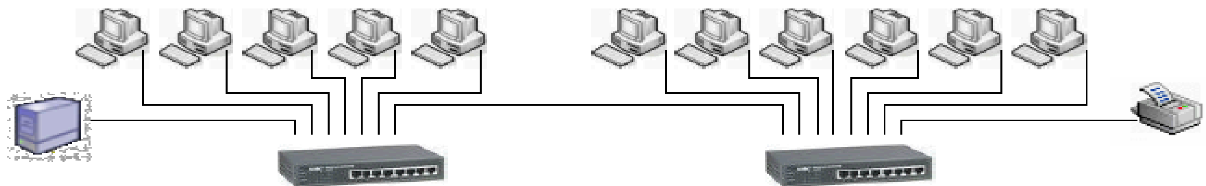


2.2. Topologie en étoile



La topologie en étoile est, de loin, la plus fréquente. Chaque unité est reliée à un nœud central (HUB ou SWITCH) par l'intermédiaire d'un câble à paires torsadées. Les connecteurs sont de type RJ45.
Le HUB est également appelé concentrateur.
Le SWITCH est également appelé commutateur.

Les HUBS ou SWITCHS peuvent être montés en cascade pour former des structures plus complexes :



Les switchs peuvent être reliés par fibre optique (distance importante, vitesse de transmission…)

2.3. Comparaison des trois topologies de base

Topologie en bus
Une topologie en bus est la mieux adaptée dans les cas suivants :
- ✓ le réseau est de petite taille,
- ✓ on recherche avant tout la solution la moins onéreuse,
- ✓ la configuration du réseau est figée (câblage, connectique),
- ✓ le réseau ne sera pas amené à s'étendre de manière importante.

Topologie en étoile
Une topologie en étoile est cependant préférable lorsque vous vous situez dans l'un des cas ci-dessous :
- ✓ la reconfiguration est très importante (ajout, retrait d'une station dans la topologie),
- ✓ vous voulez identifier rapidement les problèmes de dysfonctionnement réseau,
- ✓ le réseau comporte un nombre important de noeuds,
- ✓ la configuration réseau est susceptible d'évoluer radicalement dans le futur.

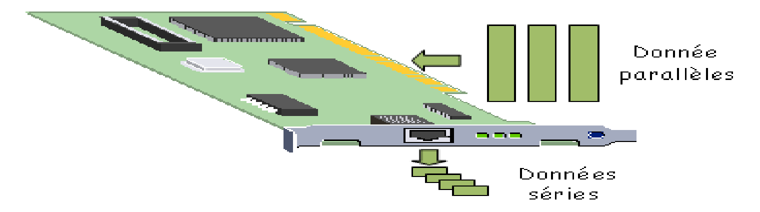
Topologie en anneau
Une topologie en anneau est finalement conseillée dans les cas évoqués ci-dessous :
- ✓ les temps de réponses ne doivent pas se dégrader même si la charge réseau est élevée,
- ✓ un réseau à haute vitesse est requis,
- ✓ la configuration réseau est relativement figée et ne risque pas d'évoluer de manière importante.

III . Les équipements réseau

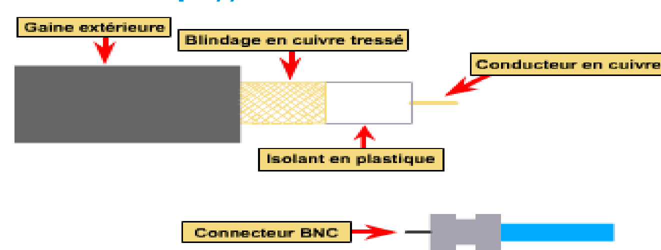
Un réseau est constitué d'ordinateurs reliés par un ensemble d'éléments matériels et logiciels. Les éléments matériels permettant d'interconnecter les ordinateurs sont les suivants:
- **La carte réseau** (parfois appelé *coupleur*): il s'agit d'une carte connectée sur la carte-mère de l'ordinateur et permettant de l'interfacer au support physique, c'est-à,-dire au lignes physiques permettant de transmettre l'information
- **La prise et le connecteur** : il s'agit des éléments permettant de réaliser la jonction mécanique entre la carte réseau et le support physique
- **Le support physique d'interconnexion**: c'est le support (généralement filaire, c'est-à-dire sous forme de câble) permettant de relier les ordinateurs entre eux. Les principaux supports physiques utilisés dans les réseaux sont les suivants:
  - Le câble coaxial
  - La paire torsadée
  - La fibre optique
- **Les équipements d'interconnexion des réseaux.**

3.1 . Cartes Réseaux
Les cartes réseaux sont installées dans un connecteur (slot) d'extension sur chaque ordinateur et serveur du réseau, ils réalisent la connexion physique entre l'ordinateur et le câble réseau.
Les fonctions assurées par la carte réseau sont les suivantes :
- préparation pour le câble réseau des données qui seront transmises à partir de l'ordinateur.
- envoi des données vers un autre ordinateur.
- contrôle du flux de données entre l'ordinateur et le système de câblage.

Une carte réseau contient le matériel et les microprogrammes qui mettent en œuvre les fonctions LLC (Logical Link Control) et MAC (Medium Access Control).



3.2 . Câbles réseaux
Le choix d'un câblage peut s'avérer compliqué. Belden, un des premiers fabricants de câbles, publie un catalogue de plus de 2200 types de câbles dont trois groupes principaux sont les plus utilisés :
- Câble coaxial
- Paire torsadée
- Fibre optique



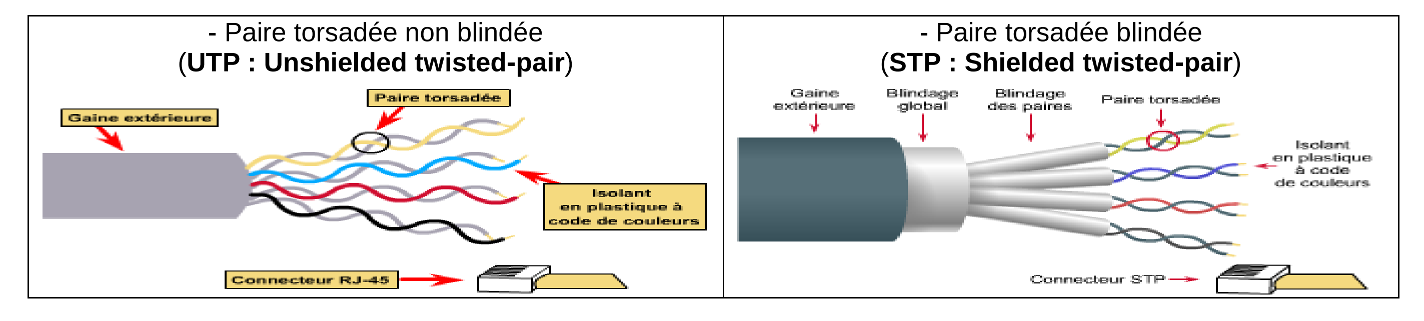
a . Câble coaxial

Il est composé d'un conducteur central en cuivre à un fil entouré d'une enveloppe isolante, d'un blindage tressé et d'une gaine externe, il existe aussi des variantes à double et à quatre blindages.

b . Paire torsadée

Une paire torsadée est constituée de deux brins torsadés en cuivre, protégés chacun par une enveloppe isolante, on distingue :

- Paire torsadée non blindée (**UTP : Unshielded twisted-pair**)	- Paire torsadée blindée (**STP : Shielded twisted-pair**)

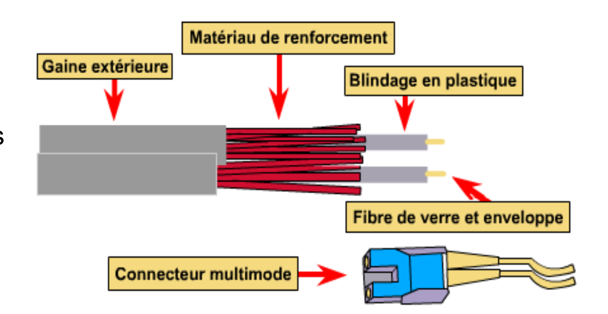


c . Fibre Optique

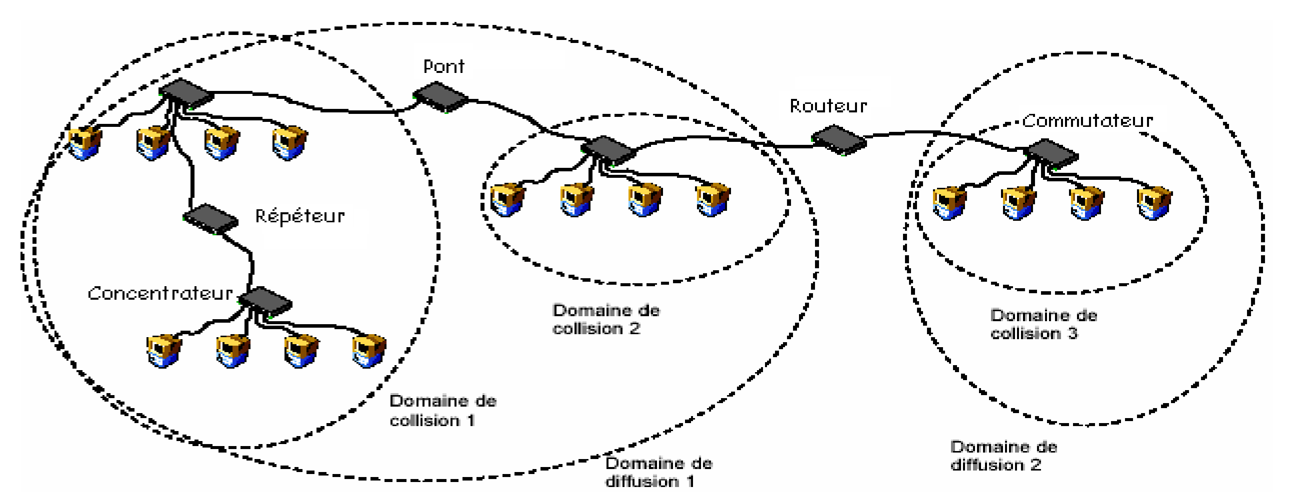
La fibre est constituée d'un cylindre en verre,ou parfois en plastique, extrêmement fin, appelé brin central, entouré d'une couche de verre appelé gaine optique.

- Elles véhiculent des signaux sous forme d'impulsions lumineuses
- Chaque fibre de verre transmet les signaux dans un seul sens.

De ce fait, un câble est constitué de deux fibres. Une pour l'émission et l'autre pour la réception.



3.3. Equipements d'interconnexion des réseaux



Définitions des principaux équipements d'interconnexion des réseaux.

- Répéteur : Dispositif matériel permettant d'étendre l'utilisation d'un média (fibre optique, câble coaxial...) au-delà de ses capacités normales, en réémettant le signal et en l'amplifiant.
- Le concentrateur (Hub) : Point de connexion commun aux d'un réseau. Un concentrateur comporte plusieurs ports. Lorsque les données arrivent à l'un des ports, elles sont copiées vers les autres ports de sorte que tous les périphériques du réseau local puissent voir les données.
- Concentrateur à commutation (switch) : Périphérique réseau central (concentrateur multiport) qui transfère les paquets vers des ports spécifiques et non vers tous les ports. De cette manière, les connexions entre les ports proposent la bande passante la plus large disponible.
- Le pont : Équipement transférant des données d'un réseau à un autre sans les modifier, en utilisant le même lien, mais pas les mêmes protocoles.
- Le Routeur : Matériel spécialisé ou ordinateur équipé de logiciels adéquats, assurant la transmission de données entre plusieurs réseaux.
- La Passerelle : Système logiciel et/ou matériel gérant le passage d'un environnement réseau à un autre, en assurant la conversion des données d'un format à l'autre.

- Le Modem : (modulateur/démodulateur) : Périphérique qui permet de transmettre des informations d'un ordinateur à l'autre via une ligne téléphonique. Le modem émetteur transforme les données informatiques numériques en signaux analogiques pouvant être acheminés par une ligne téléphonique. Le modem récepteur transforme les signaux analogiques en signaux numériques.

Représentation symbolique des principaux équipements d'interconnexion des réseaux.











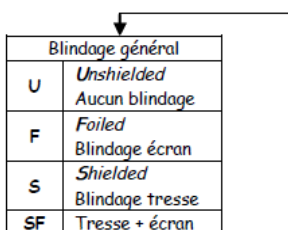
IV . Le câblage

4.1. Les câbles à paires torsadées (Twisted Pair)

Une paire torsadée est formée de **2** conducteurs enroulés en hélice l'un autour sur l'autre.
Cette configuration a pour but de maintenir précisément la distance entre les deux fils et de diminuer la diaphonie.
Un câble à paires torsadées est constitué de plusieurs paires.
Les câbles employés pour réaliser les liaisons d'un réseau local informatique (topologie étoile) sont constitués de **4** paires torsadées.
Les câbles à paires torsadées sont souvent blindés pour limiter les interférences. Le blindage peut être appliqué à l'ensemble du câble mais il peut également être appliqué individuellement à chacune des paires constituant le câble. Lorsque le blindage est appliqué à l'ensemble, on parle d'écrantage et la feuille métallique formant le blindage est appelée écran.

4.1.1. Types de blindages et appellations associées

Dénomination officielle récente : X X / Y Z Z (voir exemples ci-dessous)



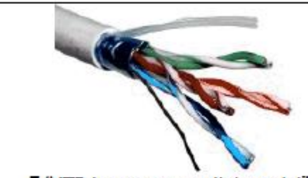
Blindage général	
U	*Unshielded* Aucun blindage
F	*Foiled* Blindage écran
S	*Shielded* Blindage tresse
SF	Tresse + écran

Blindage par paire	
U	*Unshielded* Aucun blindage
F	*Foiled* Blindage écran

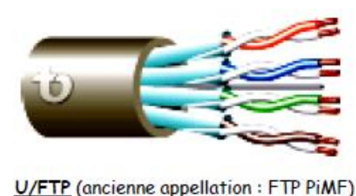
Type de paire	
TP	*Twisted Pair* Paires torsadées
TQ	*Twisted Quad* Structure en quartes



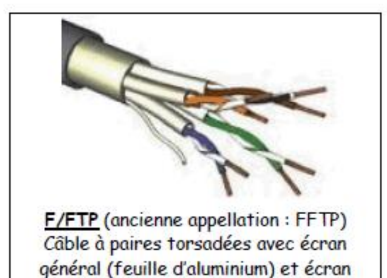
U/UTP (ancienne appellation : UTP) Câble à paires torsadées non écranté. Il est utilisé dans la téléphonie mais plus rarement dans un réseau local informatique.



F/UTP (ancienne appellation : FTP) Câble à paires torsadées proposant un blindage général réalisé par une feuille d'aluminium. Il est utilisé en téléphonie et en informatique.



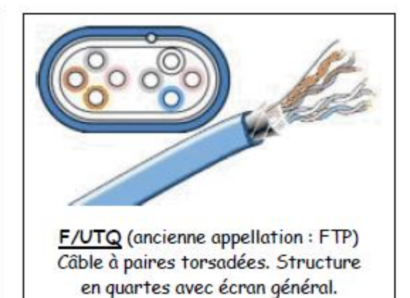
U/FTP (ancienne appellation : FTP PiMF) Câble à paires torsadées sans blindage général mais dans lequel chaque paire est écrantée individuellement.



F/FTP (ancienne appellation : FFTP) Câble à paires torsadées avec écran général (feuille d'aluminium) et écran par paire.



S/FTP (ancienne appellation : SFTP) Câble à paires torsadées avec blindage général (tresse de cuivre) et écranté par paire.



F/UTQ (ancienne appellation : FTP) Câble à paires torsadées. Structure en quartes avec écran général.

SF/UTP : Câble à paires torsadées. Blindage composé d'une tresse associée à une feuille d'aluminium.

4.1.2. Catégories de câbles

Les câbles de télécommunication sont classés en différentes catégories définissant principalement la qualité d'intégrité du signal transmis.
Certaines catégories (1 à 4) ne sont plus d'actualité car plus utilisées.

- Catégorie 5 :
  Cette catégorie définit un type de câblage autorisant une bande passante de 100 MHz. Ce standard permet l'utilisation du 100base-TX et 1000base-TX, ainsi que diverses applications de téléphonie ou de réseau.
  Dans la norme actuelle, seules les catégories 5e et 6 sont décrites.
- Catégorie 5e / classe D :
  La catégorie 5e (enhanced) définit un type de câblage autorisant une bande passante de 100MHz. Cette norme est une adaptation de la catégorie 5.
- Catégorie 6 / classe E :
  La catégorie 6 définit un type de câblage permettant une bande passante à 250 MHz et plus.
- Catégorie 6a /classe Ea :
  Ratifiée le 8 février 2008, la norme 6a est une extension de la catégorie 6 avec une bande passante de 500 MHz (norme ANSI/TIA/EIA-568-B.2-10). Cette norme permet le fonctionnement du 10GBASE-T sur 100 mètres.
  Exemple du nombre de torsades par paire mesuré sur un câble de catégorie 6a :
    Bleu / bleu-blanc : 55 tours/m
    Vert / vert-blanc : 50 tours/m
    Orange / orange-blanc : 43 tours/m
    Marron / marron-blanc : 33 tours/m
- Catégorie 7 / classe F :
  La catégorie 7 définit un type de câblage permettant une bande passante de 600 MHz.
- Catégorie 7a / classe Fa :
  La catégorie 7a permet une bande passante de 1 GHz (en cour d'étude).

4.2. Les connecteurs

C'est le connecteur RJ45 (Registered Jack) qui est le plus couramment utilisé en terminaison d'un câble à paires torsadées. Il comporte 8 broches de connexion électrique (voir numérotation ci-contre).
Il est souvent associé au standard **TIA/EIA-568-B** qui décrit le brochage de terminaison du câble.
Utilisé très couramment dans les réseaux informatiques câblés en étoile (type Ethernet), on le retrouve également en téléphonie.



4.3. Les câbles RJ45

Lorsqu'un poste de travail est connecté à un HUB (concentrateur) ou un SWITCH (commutateur), il faut utiliser un câble droit. Lorsque deux postes sont reliés directement, il faut utiliser un câble croisé. Certains équipements réseau récents sont toutefois capables de faire du (dé)croisement automatique en fonction du type de câble (MDI/MDI-X).

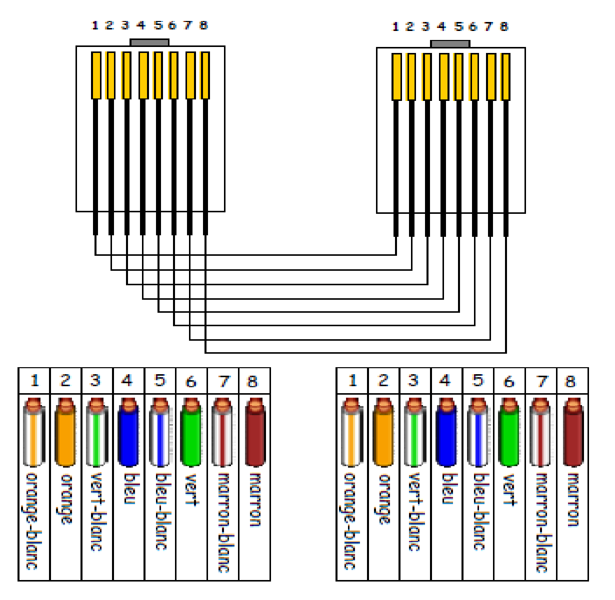
4.3.1. Norme de couleur et câblage T568A et T568B

La norme détermine 4 numéros de paire associés chacun à une couleur :
Paire 1 bleu, paire 2 orange, paire 3 vert, paire 4 marron.

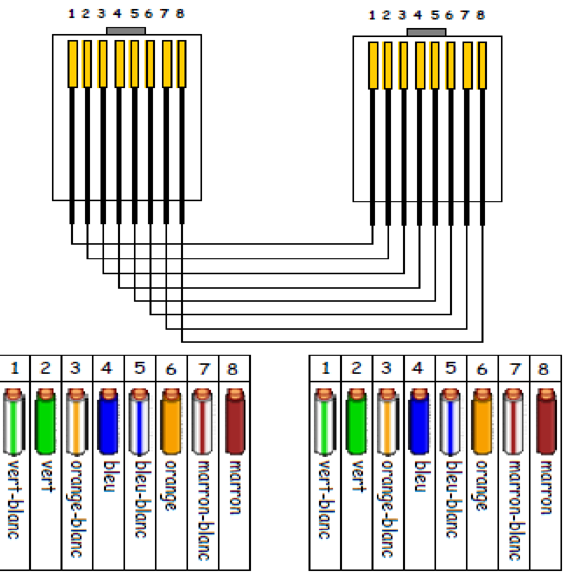
	Norme T568A		Norme T568B		
pin	couleur	paire	paire	couleur	pin
8	marron	4	4	marron	8
7	marron-blanc			marron-blanc	7
6	orange	2	3	vert	6
5	bleu-blanc	1	1	bleu-blanc	5
4	bleu			bleu	4
3	orange-blanc	2	3	vert-blanc	3
2	vert	3	2	orange	2
1	vert-blanc			orange-blanc	1

4.3.2. Câblage droit

Il existe des câbles droits câblés selon la norme T568A et d'autres selon la norme 568B. L'important est que les deux extrémités soient câblées selon la même norme.



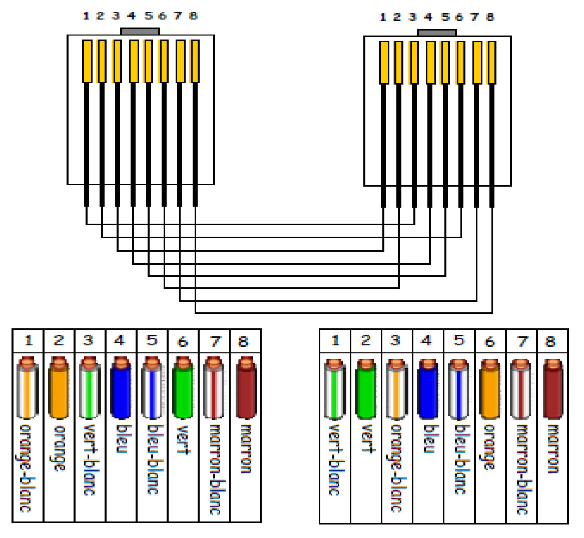
Norme 568B



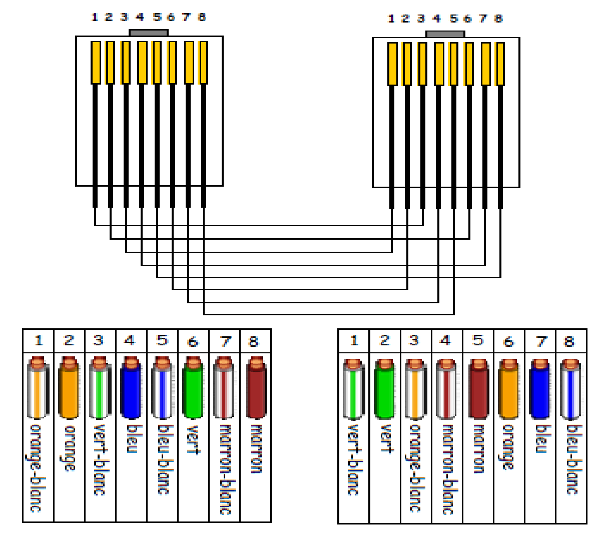
Norme T568A

4.3.3. Câblage croisé

Il existe deux types de câbles croisés. Ceux utilisés dans les réseaux 10Mbps et 100Mbps qui ne croisent que les paires 2 et 3 et ceux utilisés en 1Gbps qui croisent les 4 paires.



Câble croisé en 10base-T et 100base-T



Câble croisé en 1000base-T

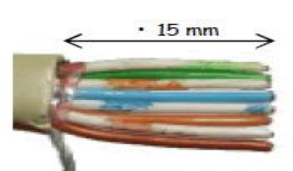
4.3.4. Fabrication d'un câble.

La fabrication d'un câble réseau n'est pas très fréquente, elle peut rendre service dans certains cas. C'est une opération minutieuse et quelques règles doivent être respectées. Les outils indispensables sont la pince coupante et la pince à sertir (RJ45).





Dénuder la gaine du câble.



Dépairer, trier les conducteurs selon le câblage désirer (ici 568A) et recouper.



Insérer à fond dans le connecteur RJ45

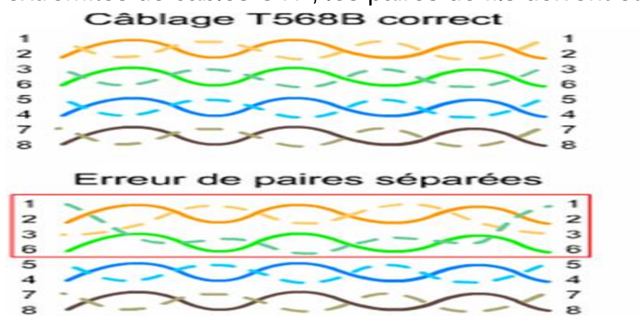


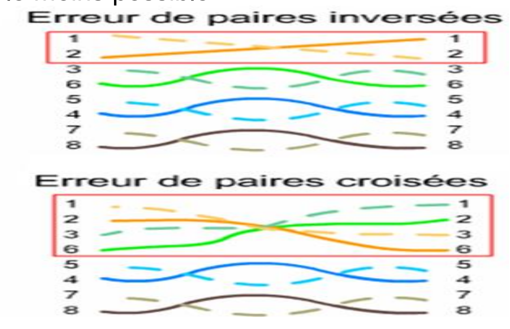
Sertir à l'aide de la pince

4.3.5. Erreurs de câblage sources de bruit

La diaphonie est la transmission des signaux d'un fil à un autre fil proche. Les câbles à paires torsadées sont conçus pour tirer parti des effets de la diaphonie afin de réduire au maximum le bruit. Si le câblage est correct ce bruit peut aisément être détecté et filtré au niveau du récepteur.

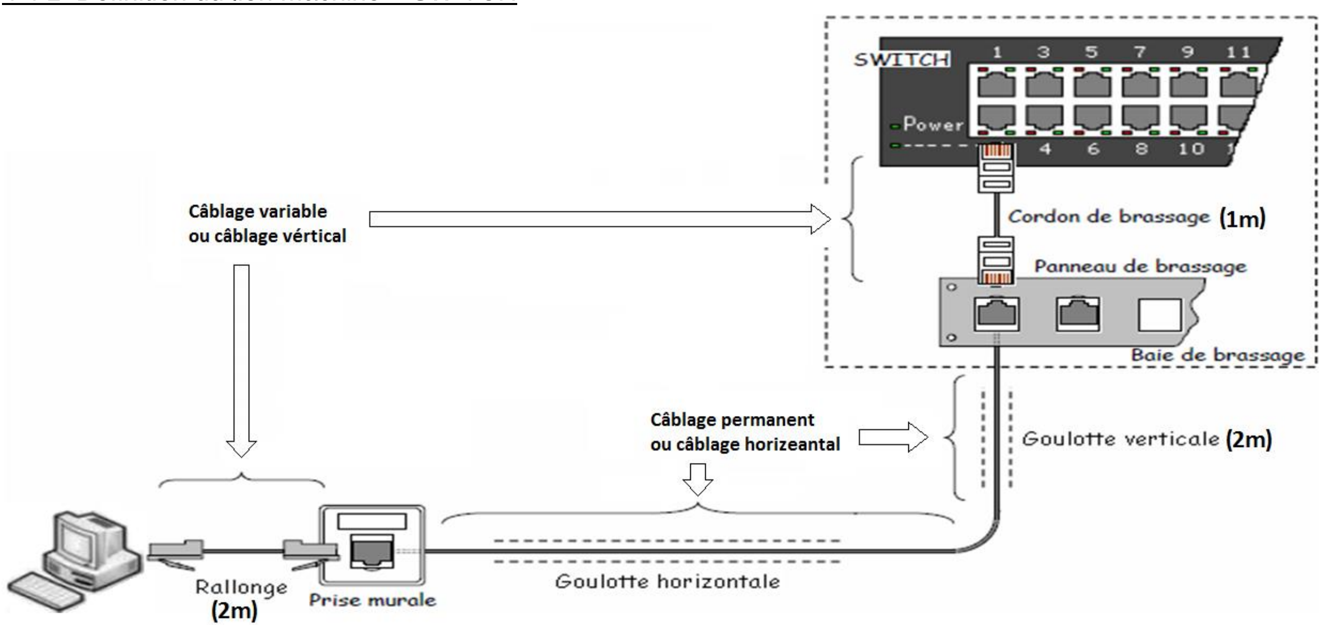
Les câbles UTP des catégories supérieures sont dotés de paires aux torsades plus nombreuses afin de réduire la diaphonie pour les fréquences de transmission élevées. Lorsque les connecteurs sont raccordés aux extrémités de câbles UTP, les paires de fils doivent être détorsadées le moins possible.





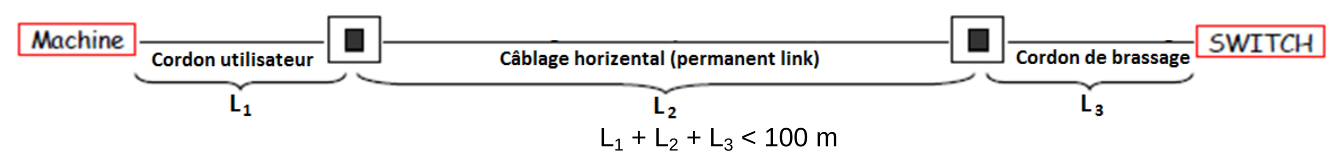
4.4. Réalisation d'un câblage réseau (pré-câblage **VDI**)

4.4.1. Définition du lien machine – SWITCH



Les besoins en communications d'aujourd'hui induisent la nécessité d'un pré-câblage VDI (Voix Données Images) à l'intérieur ou entre les différents bâtiments d'une même enceinte.

- Les liaisons entre bâtiments sont très souvent réalisées à l'aide de fibres optiques pour des raisons de longueur de liaison.
- Les liaisons internes adoptent la plupart du temps la topologie en étoile et sont réalisées par l'intermédiaire de câbles à paires torsadées. La norme impose une longueur maximale de câblage entre la machine et le SWITCH de 100 m.



$L_1 + L_2 + L_3 < 100$ m

$L_1 + L_3 < 10$ m (câblage vertical : cordon utilisateur(rallonge) + cordon de brassage ou patch cord)

$L_2 < 90$ m (câblage horizontal / permanent link)

Dans la plupart des cas $L_1 < 5$m et $L_2 < 5$m

Pour assurer une bonne liaison, des précautions de câblage doivent être respectées :

Le câble doit être déroulé (utiliser un dérouleur de câble)
Eviter de marcher sur les câbles ou d'y déposer des objets lourds.
Rayon de courbure minimal durant l'installation : 31 mm
Rayon de courbure minimal, installation terminée : 62 mm

Eviter de serrer les colliers de fixation, le câble doit pouvoir coulisser légèrement.
Les courants forts et courants faibles doivent cheminer dans des conduits différents. Des distances minimales doivent également être respectées entre les deux câblages. Ces distances dépendent du type de câble utilisé (exemples : 5 cm minimum en solution STP/FTP et 20 cm en UTP)
Détorsadage des paires : 13 mm maximum en catégorie 5
L'écran ou le blindage du câble doit être conservé au plus près possible de la connexion.
Mise à la terre du blindage des câbles et des baies de brassage.

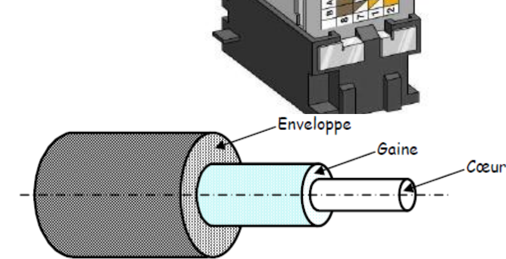
Densité préconisée de pré-câblage des postes de travail potentiels :
2 postes par bureau
1 poste tous les 2,5 m
1 poste pour 6 m^2 utile

4.4.2. Connexion d'une embase RJ45 (modular plug femelle)

Il existe de nombreux modèles d'embases RJ45. L'exemple proposé ici est une embase de catégorie 5 ne nécessitant pas l'utilisation d'outils particuliers pour sont câblage. Les contacts sont auto-sertissants. Les normes T568 A et B sont toujours rappelées sur le boîtier.
Détorsadage maximum 13 mm pour la catégorie 5 !

4.5. La fibre optique

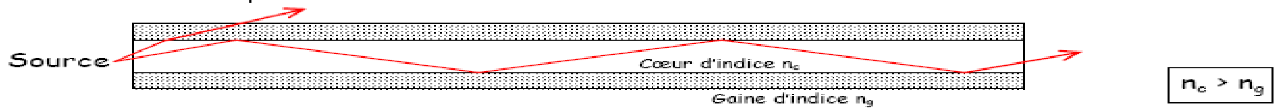
La fibre optique est un guide optique cylindrique en verre d'un diamètre de 10 à 300 µm, recouvert d'une gaine de diamètre compris entre 100 et 400 µm. Le tout est recouvert d'une enveloppe de protection en polymère.



Avantages de la fibre optique :
Très large bande passante. Cela permet le multiplexage de nombreux canaux sur un même support (Audio, données, images …)
Faible volume et grande légèreté.
Très faible atténuation (aux alentours de 0,2 dB/Km). Les points de régénération peuvent être espacés de plusieurs dizaines de kilomètres, voire centaines de kilomètres.
Excellente qualité de transmission (insensibilité aux perturbations électromagnétiques)
Bonne résistance aux températures.
Matière première bon marché (silice)
Difficultés d'emploi :
Problèmes de raccordement (pertes > 1dB)
Dérivations difficiles.

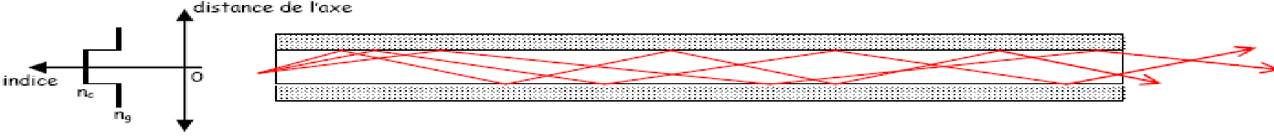
4.5.1. Principe de fonctionnement

La fibre optique est un guide d'onde qui exploite les propriétés réfractrices de la lumière.
Le cœur de la fibre a un indice de réfraction légèrement plus élevé que la gaine. Une partie des rayons lumineux est ainsi emprisonnée dans la fibre et transmise d'un bout à l'autre.

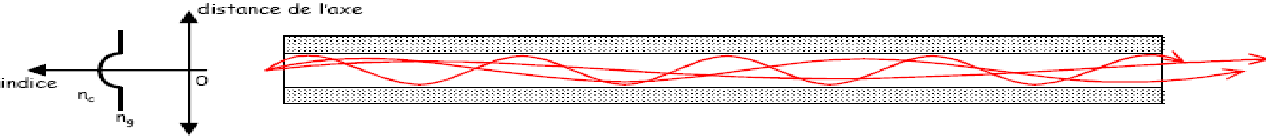


4.5.2. Fibre optique multimodes à saut d'indice (50 MHz sur 1 Km)

Ce type de fibre est qualifié de multimodes car tous les rayons lumineux ne parcourent pas la même distance à l'intérieur du coeur.

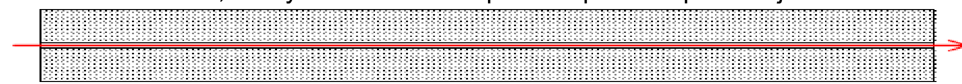


4.5.3. Fibre optique multimodes à gradient d'indice (500 MHz à 1 GHz sur 1Km)



4.5.4. Fibre optique monomode (Plusieurs GHz sur 1 Km mais plus complexe à réaliser)

Le diamètre du coeur étant très faible, le rayon lumineux ne peut emprunter qu'un trajet.



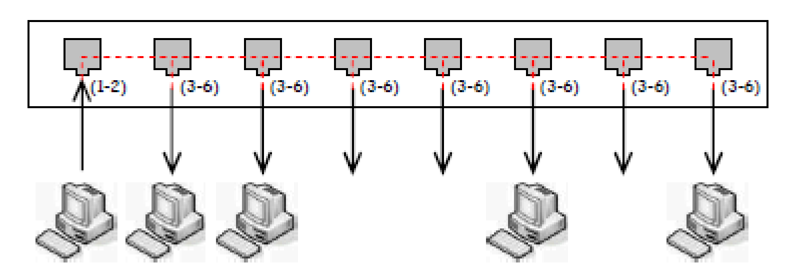
V . Switch et hub

Les hubs ou switchs sont les nœuds centraux de la structure physique en étoile d'un réseau local. Ils permettent le cheminement des données à l'intérieur du réseau entre les différentes machines qui leur sont connectées. Toutefois leur fonctionnement interne diffère.

5.1. Hub (concentrateur)

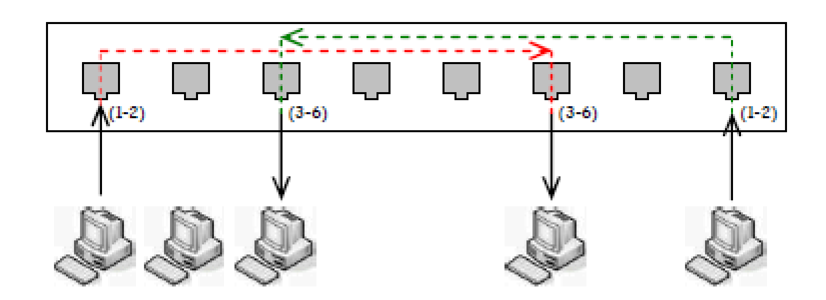
En utilisant un concentrateur (hub en anglais), chaque équipement qui lui est rattaché partage le même domaine de diffusion. Ce dispositif est un simple répéteur de données. C'est une extension du câblage.
Toute donnée entrante est répétée en sortie sur la totalité de ses ports.
Le hub possède 2 types de port :

- Port de connexion des machines
- Port d'extension (croisé) pour connecter à un autre hub



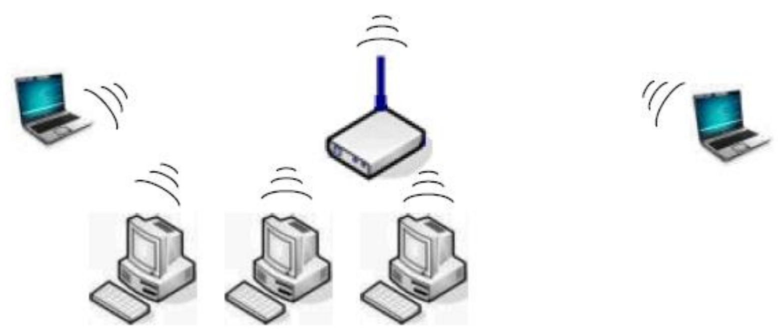
5.2. Switch (commutateur)

Un commutateur (switch en anglais) a la même apparence qu'un hub. Mais il ne se contente pas de reproduire sur tous les ports chaque trame qui lui est envoyé. Il sait déterminer sur quel port il doit envoyer une trame en fonction de l'adresse de destination.



VI. Liaisons sans fil

La technologie WiFi (Wireless Fiddelity) permet la mise en place d'un réseau sans fil. Elle utilise des fréquences radio à la place des câbles pour transmettre des données.
Le WiFi est basé sur la norme 802.11 déclinée en diverses normes (802.11a, 802.11b, 802.11g …)
Toute machine désirant communiquer sur un réseau sans fil de type WiFi doit être équipée d'une carte réseau WiFi.
Le WiFi utilise différentes bandes de fréquences, autorise de multiples types d'infrastructure (avec ou sans point d'accès) et propose différents taux de transfert et distances de fonctionnement.



ANNEXE RESUMÉ : CQFS SUR LE DECODAGE DES PAQUETS ET DATAGRAMMES.

Le paquet ARP

0 — 15 16 — 31

00 01 (indique réseau Ethernet classique)		**08 00** (indique réseau IP)
06 (longueur @ MAC)	**04** (longueur @ IP)	**00 01** (pour une requête) **00 02** (pour une réponse)
(sur 6 octets) Adresse MAC de l'émetteur de la trame…		
…Suite de l'adresse MAC de l'émetteur		**Adresse IP de l'émetteur de la trame…**
…Suite de l'adresse IP de l'émetteur		**Adresse MAC du destinataire de la trame…**
…Suite de l'adresse MAC du destinataire (dans le cas d'une requête = 00 00 00 00 00 00)		
Adresse IP du destinataire de la trame (sur 4 octets)		

Le paquet IP

0 — 15 16 — 31

Version	**Lg Entête**	**Type service**	**Longueur Totale**	
Identification			**Drapeaux**	**Déplacement de fragment**
Durée de vie (TTL)		**Protocole**	**Bloc de contrôle d'entête**	
Adresse IP émetteur				
Adresse IP destinataire				
Options				**Bourrage**
: D O N N E E S :				

Protocole : ICMP(1) --- TCP(6) --- UDP(17)

Le datagramme ICMP

0 — 15 16 — 31

Type	**0 : Echo replay 8 : Echo request**	**Code**	**Checksum**
: D O N N E E S :			

Le paquet TCP

0 — 15 16 — 31

Port source								**Port de destination**
Numéro de séquence								
Numéro d'acquittement (Accusé de réception)								
Position des données	**Réservé**	**URG**	**ACK**	**PSH**	**RST**	**SYN**	**FIN**	**Fenêtre**
Checksum								**Pointeur de données urgentes**
Options								**Bourrage**
: D O N N E E S :								

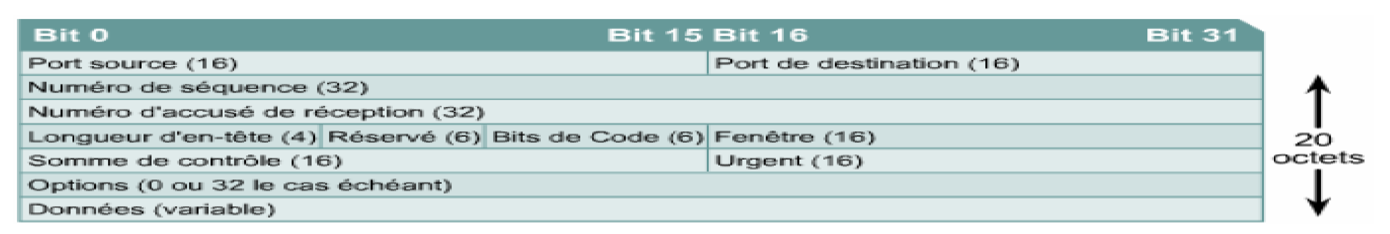
Le datagramme UDP

0 — 15 16 — 31

Port source	**Port de destination**
Taille	**Checksum**
: D O N N E E S :	

ANNEXES : DECODAGE DES PAQUETS ET DATAGRAMMES

1. Structure d'un segment TCP :



- **Port source:** numéro du port qui envoie les données.
- **Port de destination:** numéro du port qui reçoit les données.
- **Numéro de séquence:** numéro d'ordre de chaque segment.
- **Numéro d'accusé de réception:** octet TCP suivant attendu.
- **HLEN:** nombre de mots de 32 bits contenus dans l'en-tête.
- **Réservé:** champ réglé sur zéro.
- **Bits de code:** fonctions de contrôle (l'ouverture et la fermeture d'une session).
- **Fenêtre:** nombre d'octets que l'émetteur acceptera.
- **Somme de contrôle:** somme de contrôle des champs de données et d'en-tête.
- **Pointeur d'urgence:** indique la fin des données urgentes.
- **Option:** p.ex. : la taille maximale d'un segment TCP (MSS – Maximum Segment Size)
- **Données:** données de protocole de couche supérieure.

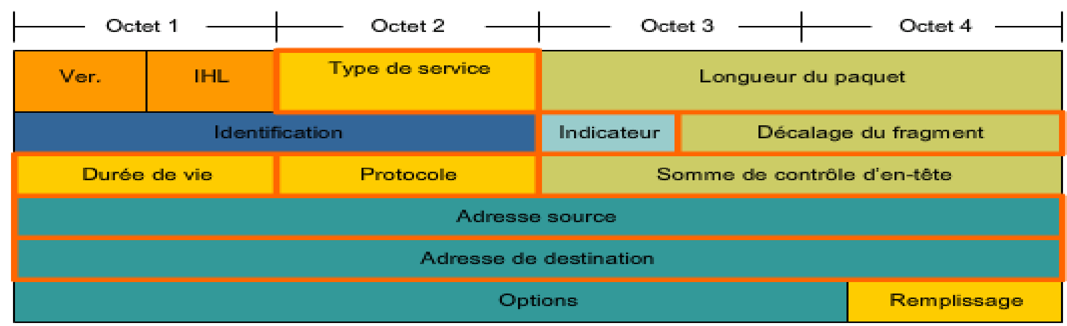
2. Structure d'un segment UDP :



- **Port source:** numéro du port qui envoie les données.
- **Port de destination:** numéro du port qui reçoit les données.
- **Longueur:** nombre d'octets de l'en-tête et des données.
- **Somme de contrôle:** somme de contrôle des champs de données et d'en-tête.
- **Données:** données de protocole de couche supérieure.

3. Structure de l'en-tête du paquet IPv4 :

Comme l'illustre la figure, un protocole IPv4 définit de nombreux champs différents dans l'en-tête de paquet. Ces champs contiennent des valeurs binaires que les services IPv4 référencent lors de la transmission de paquets sur le réseau.



On examinera les 6 champs clés suivants :

- Adresse source IP
- Adresse de destination IP
- Durée de vie (TTL)
- Type de service (ToS)
- Protocole
- Décalage du fragment

3.1. Adresse de destination IP

Le champ d'adresse de destination IP contient une valeur binaire de 32 bits représentant l'adresse de couche réseau de l'hôte destinataire du paquet.

3.2. Adresse source IP

Le champ d'adresse source IP contient une valeur binaire de 32 bits représentant l'adresse de de couche réseau de l'hôte source du paquet.

3.3. Durée de vie

La durée de vie (TTL, Time to live) est une valeur binaire de 8 bits indiquant la durée de vie restante du paquet. La valeur TTL est décrémentée de 1 au moins chaque fois que le paquet est traité par un routeur (c'est-à-dire à chaque saut). Lorsque la valeur devient nulle, le routeur supprime ou abandonne le paquet et il est retiré du flux de données du réseau. Ce mécanisme évite que les paquets ne pouvant atteindre leur destination ne soient transférés indéfiniment d'un routeur à l'autre dans une boucle de routage. Si les boucles de routage étaient autorisées à continuer, le réseau serait encombré de paquets de données n'atteignant jamais leur destination. Décrémenter la valeur TTL à chaque saut garantit qu'elle finira par devenir nulle et que le paquet avec le champ TTL expiré sera supprimé.

3.4. Protocole

Cette valeur binaire de 8 bits indique le type de données utiles que le paquet transporte. Le champ de protocole permet à la couche réseau de transmettre les données au protocole de couche supérieure approprié.
Exemples de valeurs : 01 ICMP 06 TCP 17 UDP

3.5. Type de service

Le champ de type de service contient une valeur binaire de 8 bits utilisée pour définir la priorité de chaque paquet. Cette valeur permet d'appliquer un mécanisme de qualité de service (QS) aux paquets de priorité élevée, tels que ceux transportant des données vocales de téléphonie. Le routeur traitant les paquets peut être configuré pour déterminer le paquet à transmettre en premier en fonction de la valeur de type de service.

3.6. Décalage du fragment

Comme mentionné précédemment, un routeur peut devoir fragmenter un paquet lors de sa transmission d'un média à un autre de MTU inférieure. Lorsqu'une fragmentation se produit, le paquet IPv4 utilise le champ de décalage du fragment et l'indicateur MF de l'en-tête IP pour reconstruire le paquet à son arrivée sur l'hôte de destination. Le champ de décalage du fragment identifie l'ordre dans lequel placer le fragment de paquet dans la reconstruction.

3.7. Indicateur de fragments supplémentaires

L'indicateur de fragments supplémentaires (MF) est un seul bit du champ Indicateur utilisé avec le décalage du fragment pour la fragmentation et la reconstruction de paquets. L'indicateur de fragments supplémentaires est défini pour indiquer qu'il ne s'agit pas du dernier fragment d'un paquet. Quand un hôte récepteur reçoit un paquet avec l'indicateur MF = 1, il examine le décalage du fragment pour voir où ce fragment doit être placé dans le paquet reconstruit. Quand un hôte récepteur reçoit une trame avec l'indicateur MF = 0 et une valeur non nulle dans le champ de décalage du fragment, il place ce fragment à la fin du paquet reconstruit. Les informations de fragmentation d'un paquet non fragmenté sont toutes nulles (MF= 0, décalage du fragment = 0).

3.8. Indicateur Ne pas fragmenter

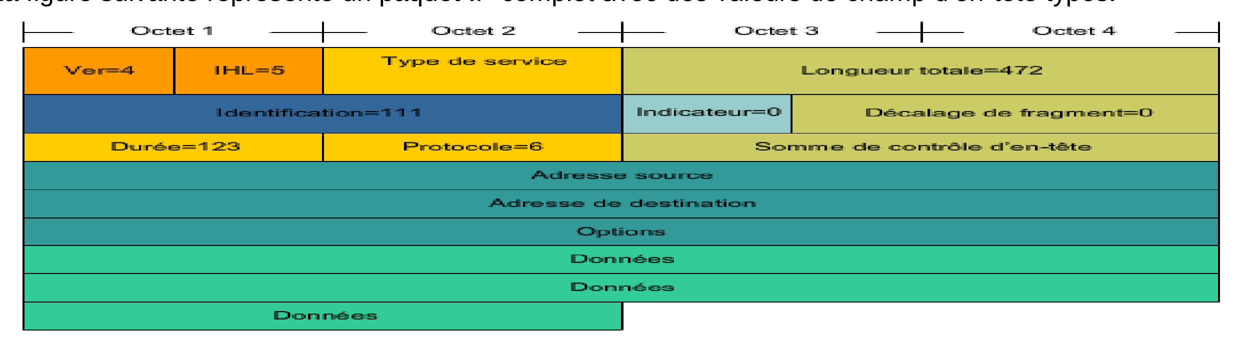
L'indicateur Ne pas fragmenter (DF) est un seul bit du champ Indicateur stipulant que la fragmentation du paquet n'est pas autorisée. Si le bit de l'indicateur Ne pas fragmenter est défini, la fragmentation de ce paquet n'est PAS autorisée. Si un routeur doit fragmenter un paquet pour permettre sa transmission descendante à la couche liaison de données mais que le bit DF est défini à 1, le routeur supprime ce paquet.

3.9. Autres champs de l'en-tête IPv4

- Version : contient le numéro de version IP (4).
- Longueur d'en-tête (IHL) : spécifie la taille de l'en-tête de paquet.
- Longueur du paquet : ce champ donne la taille du paquet entier, en-tête et données compris, en octets.
- Identification : ce champ sert principalement à identifier de manière unique les fragments d'un paquet IP d'origine.
- Somme de contrôle d'en-tête : le champ de somme de contrôle est utilisé pour vérifier l'absence d'erreurs dans l'en-tête de paquet.
- Options : des champs supplémentaires sont prévus dans l'en-tête IPv4 afin de fournir d'autres services, mais ils sont rarement utilisés.

Exemple de paquet IP

La figure suivante représente un paquet IP complet avec des valeurs de champ d'en-tête types.



- Ver = 4 : version IP.
- IHL = 5 : taille d'en-tête en mots de 32 bits (4 octets). Cet en-tête est de 5*4 = 20 octets, la taille minimale valide.
- Longueur totale = 472 : la taille de paquet (en-tête et données) est de 472 octets.
- Identification = 111 : identifiant de paquet initial (requis s'il est fragmenté par la suite).
- Indicateur = 0 : stipule que le paquet peut être fragmenté si nécessaire.
- Décalage du fragment = 0 : indique que ce paquet n'est pas fragmenté actuellement (absence de décalage).
- Durée de vie = 123 : indique le temps de traitement de la couche 3 en secondes avant abandon du paquet (décrémenté d'au moins 1 chaque fois qu'un périphérique traite l'en-tête de paquet).
- Protocole = 6 : indique que les données transportées par ce paquet constituent un segment TCP.

4. Structure d'une requête ARP/RARP :

0 - 15 bits		16 - 31 bits
Type de matériel		Type de protocole
HLen (1 octet)	PLen (1 octet)	Opération
AM expéditeur (octets 1 - 4)		
AM expéditeur (octets 5 - 6)		AP expéditeur (octets 1 - 2)
AP expéditeur (octets 3 - 4)		AM cible (octets 1 - 2)
AM cible (octets 3 - 6)		
AP cible (octets 1 - 4)		

Structure de l'en-tête RARP

Champ	Description
Type de matériel	Spécifie un type d'interface matérielle pour lequel l'expéditeur attend une réponse.
Type de protocole	Spécifie le type d'adresse de protocole de haut niveau fourni par l'expéditeur.
HLen	Longueur de l'adresse matérielle
PLen	Longueur de l'adresse de protocole
Opération	Les valeurs sont les suivantes : 1 Requête ARP 2 Réponse ARP 3 Requête RARP 4 Réponse RARP 5 Requête RARP dynamique 6 Réponse RARP dynamique 7 Erreur RARP dynamique 8 Requête InARP 9 Réponse InARP
@ Matériel de l'expéditeur	Longueur en Octet HLen
@ de Protocole de l'expéditeur	Longueur en Octet PLen
@ Matériel cible	Longueur en Octet HLen
@ Protocole cible	Longueur en Octet PLen

Exemple :

Requête RARP

1		0800_{16}
06	04	3
FE:ED:F9:23		
44:EF		non défini
non défini		FF:FF
FF:FF:FF:FF		
non défini		

Réponse RARP

1		0800_{16}
06	04	4
FE:ED:F9:23		
44:EF		192.168
10.36		FE:ED
F9:65:33:3A		
192.168.10.98		

5. Structure d'une requête BOOTP :

0 - 7 bits	8 - 15 bits	16 - 23 bits	24 - 31 bits
Op (1)	Htype (1)	HLen (1)	Hops (1)
Xid (4 octets)			
Secondes (2 octets)		Non utilisé	
Ciaddr (4 octets)			
Yiaddr (4 octets)			
Siaddr (4 octets)			
Giaddr (4 octets)			
Chaddr (16 octets)			
Nom d'hôte du serveur (64 octets)			
Nom du fichier de démarrage (128 octets)			
Zone spécifique du fournisseur (64 octets)			
Structure des messages BOOTP			

Champ	Description
Op	Code des messages (BOOTREQUEST ou BOOTREPLY)
Htype	Type d'adresse matérielle.
HLen	Longueur de l'adresse matérielle
Hops	Utilisé par le serveur pour envoyer les requêtes à un autre réseau
Xid	ID de la transaction
Secs	Secondes écoulées lors du processus.
Ciaddr	Adresse IP du client
Yiaddr	Votre adresse IP (Client)
Siaddr	@ IP du serveur servant dans le bootstrap.
Giaddr	@ IP de l'agent de relais
Chaddr	Adresse matérielle du client
Server Host Name	Le serveur qui doit fournir les informations BOOTP
Boot File Name	Fichier de démarrage suivant le SE utilisé
Vendor Specific Area	Informations facultatives sur le fournisseur.

Exemple :

Requête BOOTP :

En-tête de trame	En-tête du paquet	1	1	6	0	Vérification
Adresse MAC source	Adresse IP source	221				du CRC
FE:ED:F9:23:44:EF	Inconnu	2		Non utilisé		
Adresse MAC de destination	Adresse IP de destination	0				
FF:FF:FF:FF:FF:FF	225.225.225.225	0				
Champ Type		0				
0X8035 (Ethernet)		0				
		FE:ED:F9:23:44:EF				

Réponse BOOTP :

En-tête de trame	En-tête du paquet	2	1	6	0	Vérification
Adresse MAC source	Adresse IP source	221				du CRC
FE:ED:F9:65:33:3A	192.168.10.98	2		Non utilisé		
Adresse MAC de destination	Adresse IP de destination	0				
FE:ED:F9:23:44:EF	225.225.225.225	192.168.10.36				
Champ Type		192.168.10.97				
0X8035 (Ethernet)		192.168.10.97				
		FE:ED:F9:23:44:EF				

6. Structure d'une requête DHCP :

Elle est presque semblable à la requête BOOTP

0 - 7 bits	8 - 15 bits	16 - 23 bits	24 - 31 bits
Op (1)	Htype (1)	HLen (1)	Hops (1)
Xid (4 octets)			
Secondes (2 octets)		Indicateurs (2 octets)	
Ciaddr (4 octets)			
Yiaddr (4 octets)			
Siaddr (4 octets)			
Giaddr (4 octets)			
Chaddr (16 octets)			
Nom d'hôte du serveur (64 octets)			
Nom du fichier de démarrage (128 octets)			
Zone spécifique du fournisseur (variable)			
Structure des messages DHCP			